iBoss Enterprise Reporter

User Manual

Phantom™
Technologies
www.iboss.com

Note: Please refer to the User Manual online for the latest updates at www.ibosswebfilters.com.

Copyright © by Phantom Technologies Inc. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in chemical, manual or otherwise, without the prior written permission of Phantom Technologies Inc.

Phantom Technologies Inc makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defects. Further, this company reserves the right to revise this publication and make changes from time to time in the contents hereof without obligation to notify any person of such revision of changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

www.iBoss.com

Open Source Code

This product may include software code subject to the GNU General Public License (“GPL”), GNU Lesser General Public License (“LGPL”), or other open-source software licenses. Copies of the GPL and LGPL licenses are available upon request. You may also visit www.gnu.org to view more information regarding open-source licensing.

The GPL, LGPL and other open-source code used in Phantom Technologies Inc products are distributed without any warranty and are subject to the copyrights of their authors. Upon request, open-source software source code is available from Phantom Technologies Inc via electronic download or shipment on a physical storage medium at cost. For further details and information please visit www.iphantom.com/opensource.

Table of Contents

TABLE OF FIGURES **4**

1 ENTERPRISE REPORT MANAGER **7**

1.1 EXTERNAL ENTERPRISE REPORTER 7
1.1.1 Installing the External iBoss Enterprise Reporter on the network. *7*
1.1.2 Setup Steps to Register iBoss to External Enterprise Reporter *7*
1.2 ACCESSING THE REPORT MANAGER 8
1.3 LOGGING INTO THE REPORT MANAGER 8
1.4 REPORT GENERATION AND MANAGEMENT 9
1.4.1 Real-Time dashboard *9*
1.4.1.1 Web Dashboard 9
1.4.1.2 Bandwidth Dashboard 14
1.4.1.3 Bandwidth Plotter 18
1.4.1.4 Bandwidth Shaping 20
1.4.1.5 Threat Dashboard 24
1.4.1.6 Endpoint Security 27
1.4.2 Logs *28*
1.4.2.1 Web 29
1.4.2.2 Threats & Malware 30
1.4.3 Drop-Down Reports *32*
1.4.3.1 Report Types 34
1.4.3.2 Deleting Reports 34
1.4.3.3 Exporting PDF Reports 34
1.4.3.4 Generating a Report 34
1.4.4 Threat Controls *38*
1.4.4.1 General Settings 38
1.4.4.2 Threat Categories 40
1.4.4.3 Behavioral DLP 42
1.4.4.4 Protected Objects 43
1.4.4.5 Signature Tuning 44
1.4.4.6 Bypass IP/Port 45
1.4.5 Report Schedules *45*
1.4.5.1 Deleting Report Schedules 46
1.4.5.2 Editing Report Schedules 46
1.4.5.3 Report Schedule Processing 46
1.4.5.4 Report Schedule Types 46
1.4.5.5 Creating a Report Schedule 46
1.4.6 Automatic Desktop Monitor/Control/Record (DMCR) *52*
1.4.6.1 Installing VNC 52
1.4.6.2 Registering a Computer to DMCR 52
1.4.6.3 Video Desktop 53
1.4.6.4 Video Desktop Recordings 54
1.4.6.5 Recording Thresholds 54
1.4.7 Settings *55*
1.4.7.1 General 55
1.4.7.2 Users 64
1.4.7.3 Report Groups 66
1.4.7.4 Log Archives 67
1.4.7.5 Register Gateways 70
1.4.7.6 Time 72
1.4.7.7 Network Settings 72
1.4.7.8 SSL 73
1.4.7.9 Subscription 73
1.4.8 Report Manager System Information *74*
1.5 VIEWING REPORTS 74
1.5.1 Report Information Section *75*
1.5.1.1 Showing Report Information for Particular Users 75

1.5.1.2 Quickly switching between reports 76
1.5.2 Web Usage Statistics *76*
1.5.2.1 Web Hit Trends 77
1.5.2.2 Web Hits By Category 77
1.5.2.3 Time Use By Category 80
1.5.2.4 Top Visited Domains 82
1.5.2.5 Top Blocked Domain 82
1.5.2.6 Top Users By Category Time Use 83
1.5.2.7 Top Users By Category Web Hits 85
1.5.2.8 Top Users By Overall Web Hits 87
1.5.2.9 Top Users By Overall Time Use 88
1.5.2.10 Top Blocked Users 89
1.5.2.11 Trending Now 90
1.5.2.12 Suspicious 91
1.5.2.13 Liability 92
1.5.2.14 Filter Avoidance 93
1.5.3 Bandwidth Statistics *94*
1.5.3.1 Graph 94
1.5.3.2 Top Overall Users 95
1.5.3.3 Top Downstream Users 96
1.5.3.4 Top Upstream Users 97
1.5.3.5 Domains 98
1.5.4 Threats & Malware *99*
1.5.4.1 Top Overall Threats 99
1.5.4.2 Top Outbound Threats 100
1.5.4.3 Top Inbound Threats 101
1.5.4.4 Top User by Threats 102
2 REGULATORY STATEMENT 103

Table of Figures

Figure 1 - iBoss Reports Login 9
Figure 2 – Web dashboard 10
Figure 2 - Real-time Bandwidth Graph 11
Figure 4 – Real-Time Web Hits Graph 11
Figure 5 - Current Top Bandwidth Consumers 12
Figure 6 - Current Top Bandwidth Consumers Full List 12
Figure 3 - Real-time URL Access Activity 13
Figure 8 – Current Activity 14
Figure 9 – Bandwidth Dashboard 16
Figure 10 – Real Time Activity 16
Figure 11 –Data Movement Maps 17
Figure 12 – Real Time Bandwidth 18
Figure 13 – Real-Time Bandwidth Plotter 19
Figure 14 – Connection Detail Full List 19
Figure 15 – Bandwidth Shaping 22
Figure 16 – Downstream Bandwidth Overview 22
Figure 17 – Upstream Bandwidth Overview 22
Figure 18 – Unshaped bandwidth 23
Figure 19 – Bandwidth Pools 24
Figure 20 – Threat dashboard 25
Figure 21 – Real-Time Activity 26
Figure 22 – Threat Activity 27

Figure 23 – Endpoint Security 28
Figure 24 – Web Logs 29
Figure 25 – Web Log Search Filters 30
Figure 26 - Site Callouts 30
Figure 27 – Threats & Malware 31
Figure 28 – Threat Search Filters 32
Figure 29 – Drop-Down Reports 33
Figure 30 - Generate Report 36
Figure 31 – General Settings 39
Figure 32 – Threat Categories 41
Figure 33 – Behavioral DLP 42
Figure 34 – Protected Objects 43
Figure 35 – Signature Tuning 44
Figure 36 – Bypass IP/Port 45
Figure 37 - Report Schedules 46
Figure 38 - Create a Report Schedule 49
Figure 39 - UVNC Properties 52
Figure 40 - Video Desktop Monitoring 53
Figure 41 - Live Desktop MultiView 54
Figure 42 - Report Manager Settings 58
Figure 43 - Report Manager Database Settings 60
Figure 44 - Report Users 64
Figure 45 - Add Report Manager User 65
Figure 46 – LDAP User config 66
Figure 47 - Report Groups 66
Figure 48 - Add Reporting Group 67
Figure 49 - Manage URL Log Archives 68
Figure 50 - Manage Bandwidth Log Archives 69
Figure 51 – IPS Logs 69
Figure 52 - Register iBoss Devices 70
Figure 53 - Register Gateway 71
Figure 54 - Configure Time 72
Figure 55 - Configure IP Address Settings 72
Figure 56 - Subscription 73
Figure 57 – System Info 74
Figure 58 - Report Information Section 75
Figure 59 – Find User 76
Figure 60 - Web Usage Statistics 76
Figure 61 – Web Hit Trends 77
Figure 62 – Web Hits by Category 78
Figure 63 - Web Category Detail 79
Figure 64 - Time Use By Category 81
Figure 65 – Top Visited Domains 82
Figure 66 – Top Blocked Domains 83
Figure 67 – Top Users by Category Time Use 85
Figure 68 – Top Users by Category Web Hits 86

Figure 69 - Top Users By Overall Web Hits 87
Figure 70 - Top Users by Overall Time Use..... 88
Figure 71 – Top Blocked Users 89
Figure 72 – Trending Now..... 90
Figure 73 – Suspicious..... 91
Figure 74 – Liability 92
Figure 75 – Filter Avoidance 93
Figure 76- Graph..... 94
Figure 77 – Top Bandwidth Users 95
Figure 78 – Top Downstream Users 96
Figure 79 – Top Upstream Users 97
Figure 80 – Domains..... 98
Figure 81 – Top Overall Threats..... 99
Figure 82 – Top Outbound Threats..... 100
Figure 83 – Top Inbound Threats 101
Figure 84 – Top Users by Threats..... 102

1 Enterprise Report Manager

The iBoss is equipped with an advanced report manager capable of tracking and generating statistics and a variety of aspects of network traffic. This includes web statistics such as web sites visited and top visited domains, as well as detailed port and IP Address accesses.

The report manager provides a deep drill down capability that can identify potential risks as well as help optimize the network. The high level of report detail also includes a variety of information that can be summarized for all users in a report or information specific to a particular user. This includes bandwidth usage and graphs showing accesses throughout the report period.

The report manager is separated into two major subsections. The first deals with report management, scheduling and generation, while the other involves the report viewing.

1.1 External Enterprise Reporter

The External Report Manager or Enterprise Reporter is an appliance that offloads the reporting onto a different server appliance.

1.1.1 Installing the External iBoss Enterprise Reporter on the network.

Please configure the network settings for the external iBoss Enterprise Reporter before placing it on the network. Please refer to the Network Settings section for the Enterprise Reporter for more information on how to configure these settings.

Once the network settings have been configured, the iBoss Enterprise Reporter is ready to be installed on the network. The port you will be using is the “LAN” port located on the back of the iBoss Enterprise Reporter.

Place the iBoss Enterprise Reporter on the switch just as a computer would be. For example, add a network cable from your switch to the “LAN” port of the Enterprise Reporter. Do not put the iBoss Enterprise Reporter in line, like you would when setting up the iBoss filter.

After setting up the iBoss Enterprise Reporter on the network, do not forget to identify the Enterprise Reporter from within the iBoss Filter web interface and Select “No, Bypass Filtering Rules”.

1.1.2 Setup Steps to Register iBoss to External Enterprise Reporter

This section is a quick guide for registering iBoss devices to an Enterprise Reporter.

1. Setup an IP address for the iBoss Web Filter (please refer to the iBoss IP address section to set this)

2. Setup an IP address for the iBoss Enterprise Reporter (please refer to the iBoss Enterprise Reporter Network Settings section to set this)

3. Log into the report manager and click on Settings→ General → then change the Report Database Password. (please refer to the iBoss Enterprise Reporter Settings section for more information)

4. Click on Register iBoss Devices→ Add Device → Then set the iBoss name, iBoss IP address, iBoss Web Filter subscription key, and copy the Security key. (please refer to the iBoss Enterprise Reporter Settings section for more information)

5. Log into the iBoss device and click on Preferences → Configure Report Settings → Edit General Report Settings → change the 'Configure iBoss for' option to "External Report Manager". (please refer to the iBoss Report Settings section for more information)

6. Enter the IP address, database password, and security key of the iBoss Enterprise Reporter and click Save. (please refer to the iBoss Report Settings section for more information)

Note: Please be sure to identify the report manager within the iBoss interface to bypass any filtering rules.

1.2 Accessing the Report Manager

You can access the report manager only while on the same network as the iBoss. You can access the iBoss reports from any computer on the network that has access to the iBoss interface.

Note: The default IP address of the iBoss Enterprise Reporter is 192.168.1.20.

1.3 Logging into the Report Manager

The default username for the report manager is admin. There is no password by default.You will need to change this setting.

Additional users are created in the settings portion of the Report Manager. These users can either be local to the reporter or, if LDAP is configured, users from Active directory, eDirectory, or OpenDirectory. You can also configure specific privileges for the user to restrict the types of operations the user can perform within the report manager.

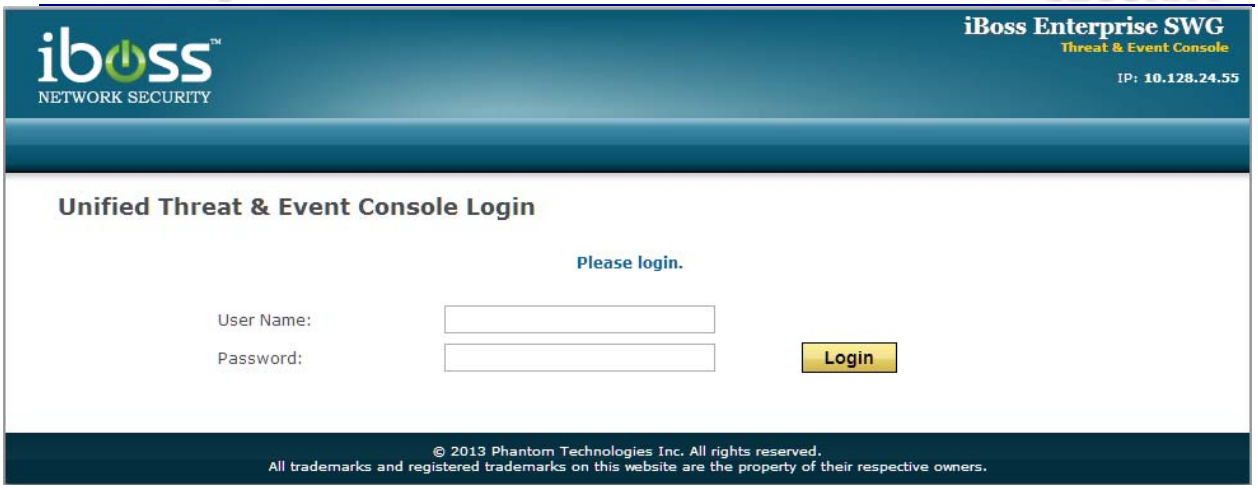


Figure 1 - iBoss Reports Login

1.4 Report Generation and Management

1.4.1 Real-Time dashboard

After logging into the report manager, the iBoss presents a page detailing the current activity. This page contains information regarding what is currently occurring on the network. There are several other sections within the report management section that include viewing and creating generated reports, viewing and creating report schedules, configuring report settings, and viewing system information.

1.4.1.1 Web Dashboard

The current activity section shows active real-time information about the network. This information is updated in real-time automatically.

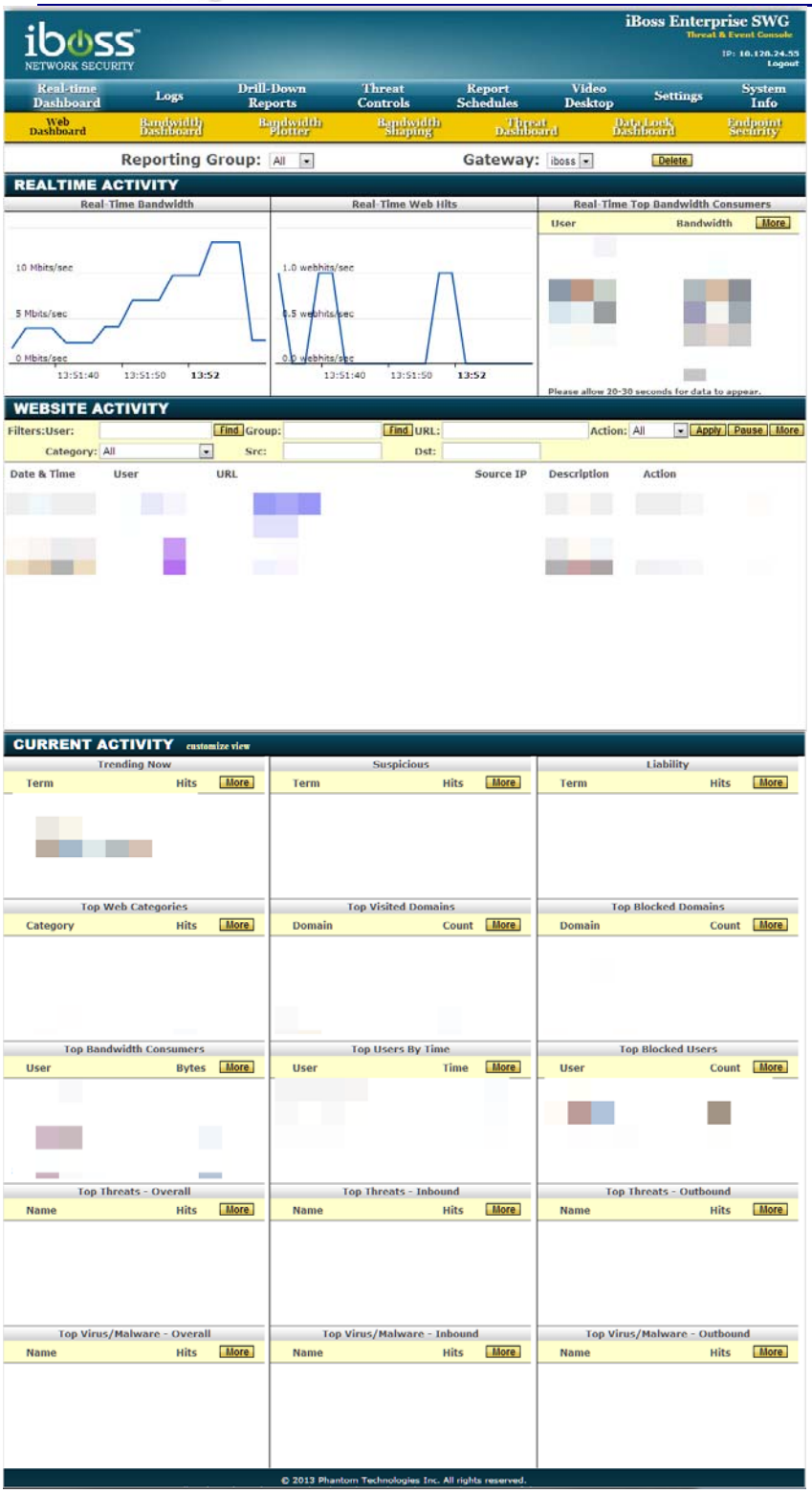


Figure 2 – Web dashboard

1.4.1.1.1 *Real-time Bandwidth Activity Graph*

The first section includes real-time Bandwidth Activity that includes Bandwidth in kilobits per second. It is necessary to hover the mouse over the graph to view the numerical data.

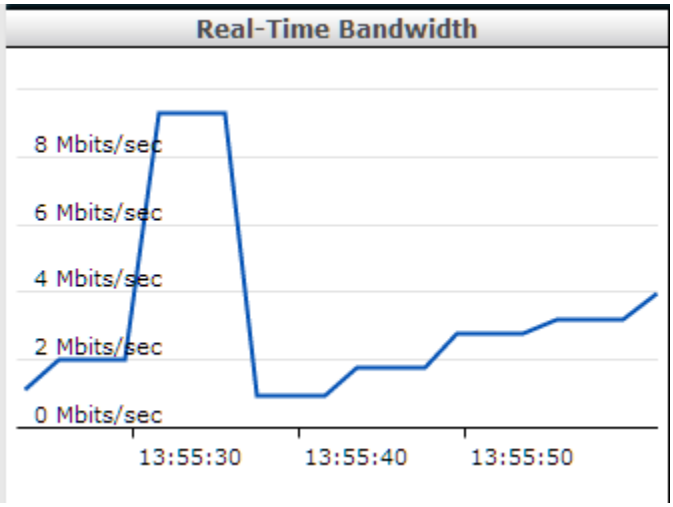


Figure 2 - Real-time Bandwidth Graph

1.4.1.1.2 *Real-Time Web Hits*

The second section is a graph indicating number of web hits. The yellow graph is the total number of web hits, where the black line is the number of blocked web hits. It is necessary to hover the mouse over the graph to get the numerical data.

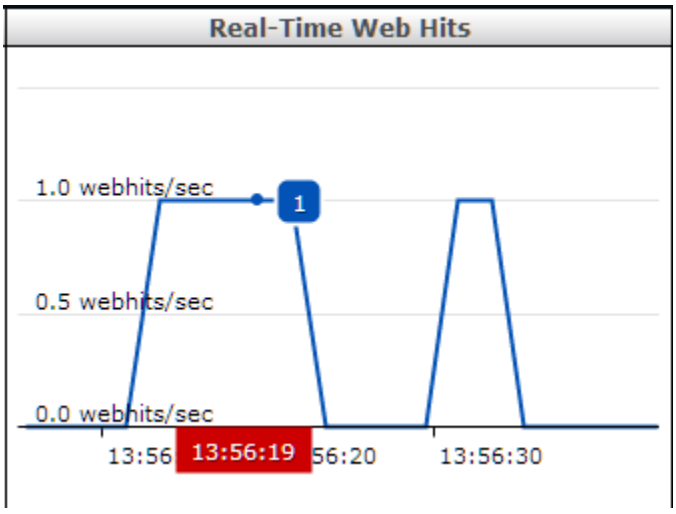


Figure 4 – Real-Time Web Hits Graph

1.4.1.1.3 *Real-Time Top Bandwidth Consumers*

This section includes the top consumers of bandwidth updated in real-time. You can click on the "**More**" button for more details of users.

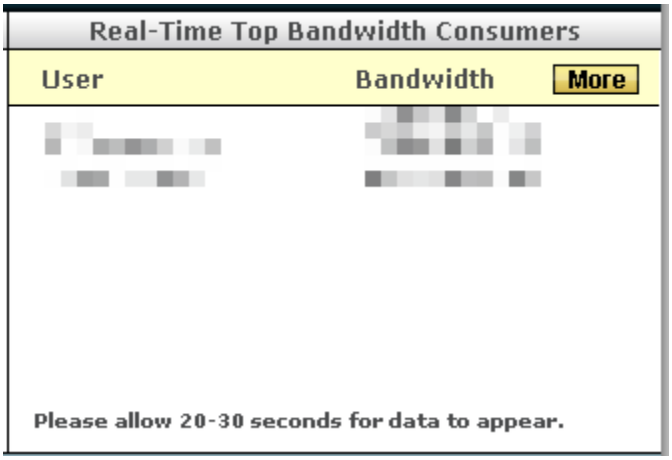


Figure 5 - Current Top Bandwidth Consumers

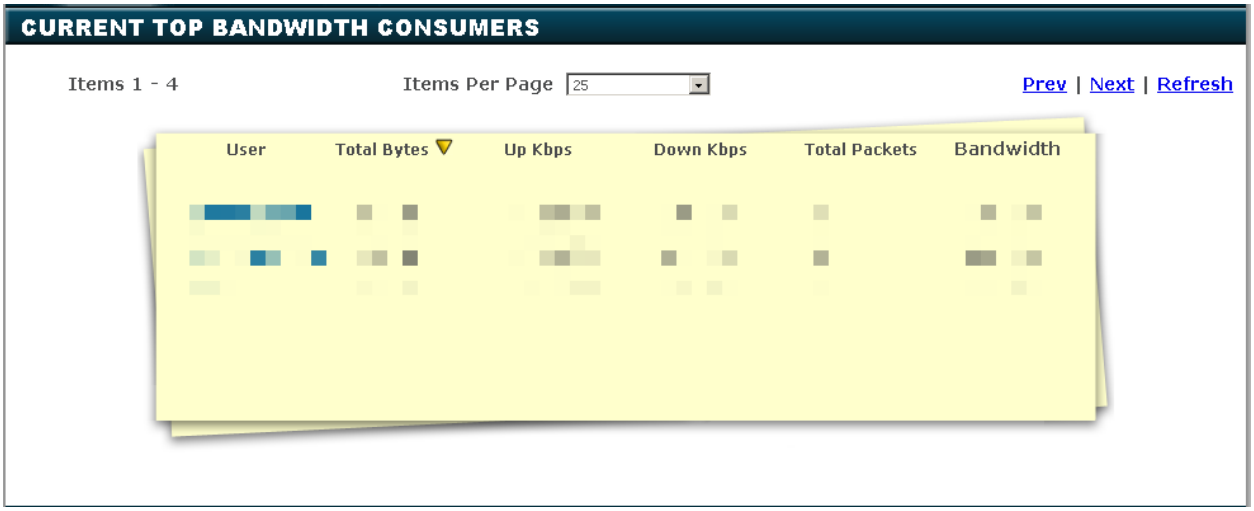


Figure 6 - Current Top Bandwidth Consumers Full List

1.4.1.1.4 *Real-time website activity*

This section shows the current websites being visited. The URLs are updated in real-time as users on the network access website destinations. It will also provide details about the URL access including categories. The list will highlight URLs that were blocked by the iBoss. This list is updated in real-time without the need to refresh the page.

This section also has a filter to only show a specific User and/or Action (Allowed or Blocked). You may simply click the username in this list to automatically set the filter to a specific user. You may also click the Pause button to stop the list from scrolling.

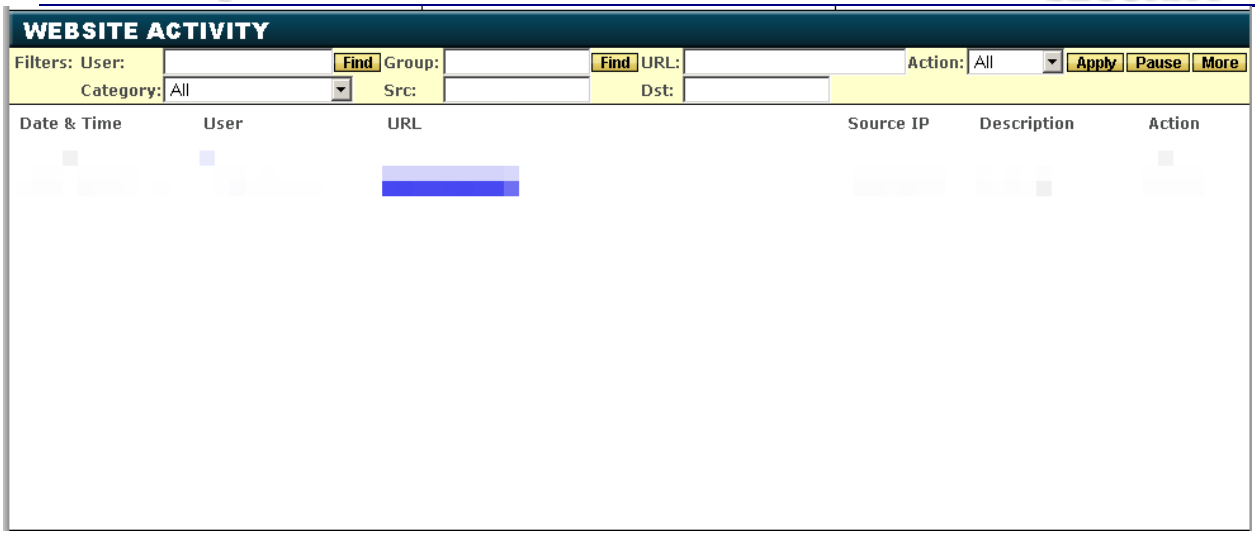


Figure 3 - Real-time URL Access Activity

1.4.1.1.5 *Current Activity*

This section provides, at a glance, information about the overall trends on the filtered network. It is divided up in to cubes, all of which can be tasked to show a different field. Fields available are:

- Trending Now
- Suspicious
- Liability
- Top Web Categories
- Top Visited Domains
- Top Blocked Domains
- Top Bandwidth Consumers
- Top Users By Time
- Top Blocked users
- Top Threats – Overall
- Top Threats – Inbound
- Top Threats – Outbound
- Top Virus/Malware – Overall
- Top Virus/Malware – Inbound
- Top Virus Malware – outbound

In addition, all of the fields have a MORE button which brings up more details about the item in question.

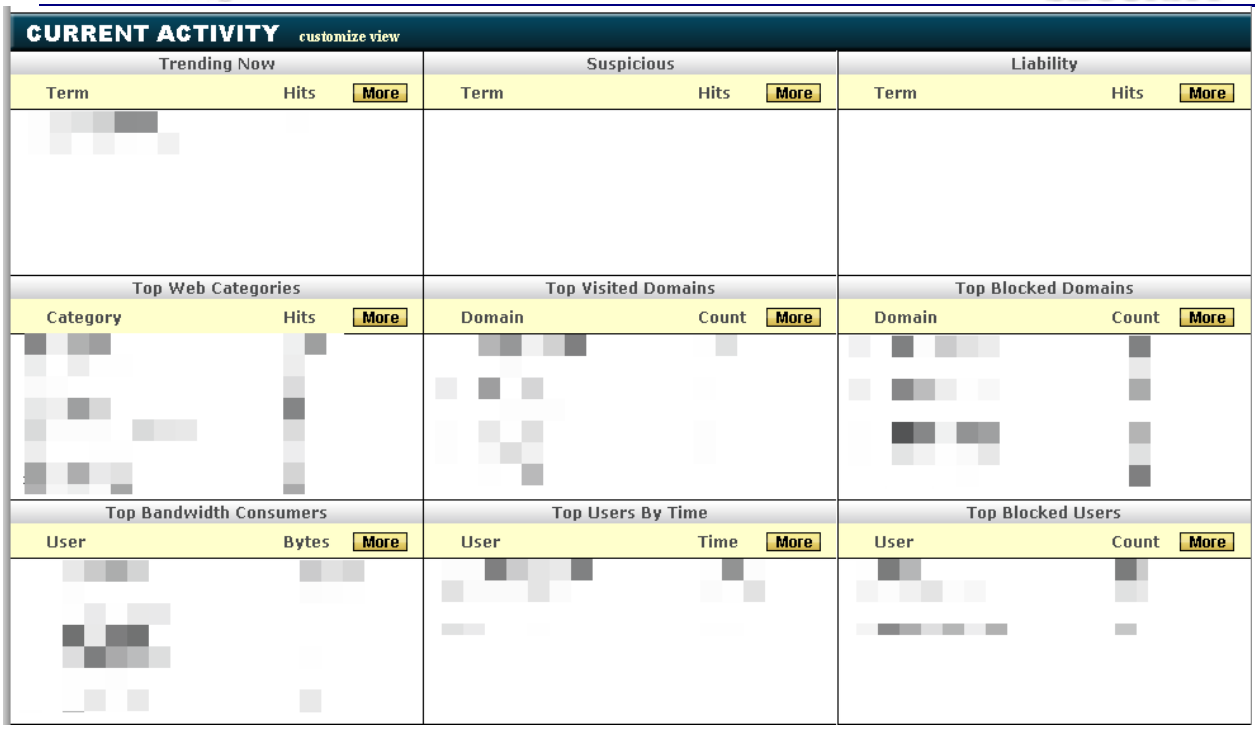


Figure 8 – Current Activity

1.4.1.2 Bandwidth Dashboard

This page allows you to view overall trends in your bandwidth usage.

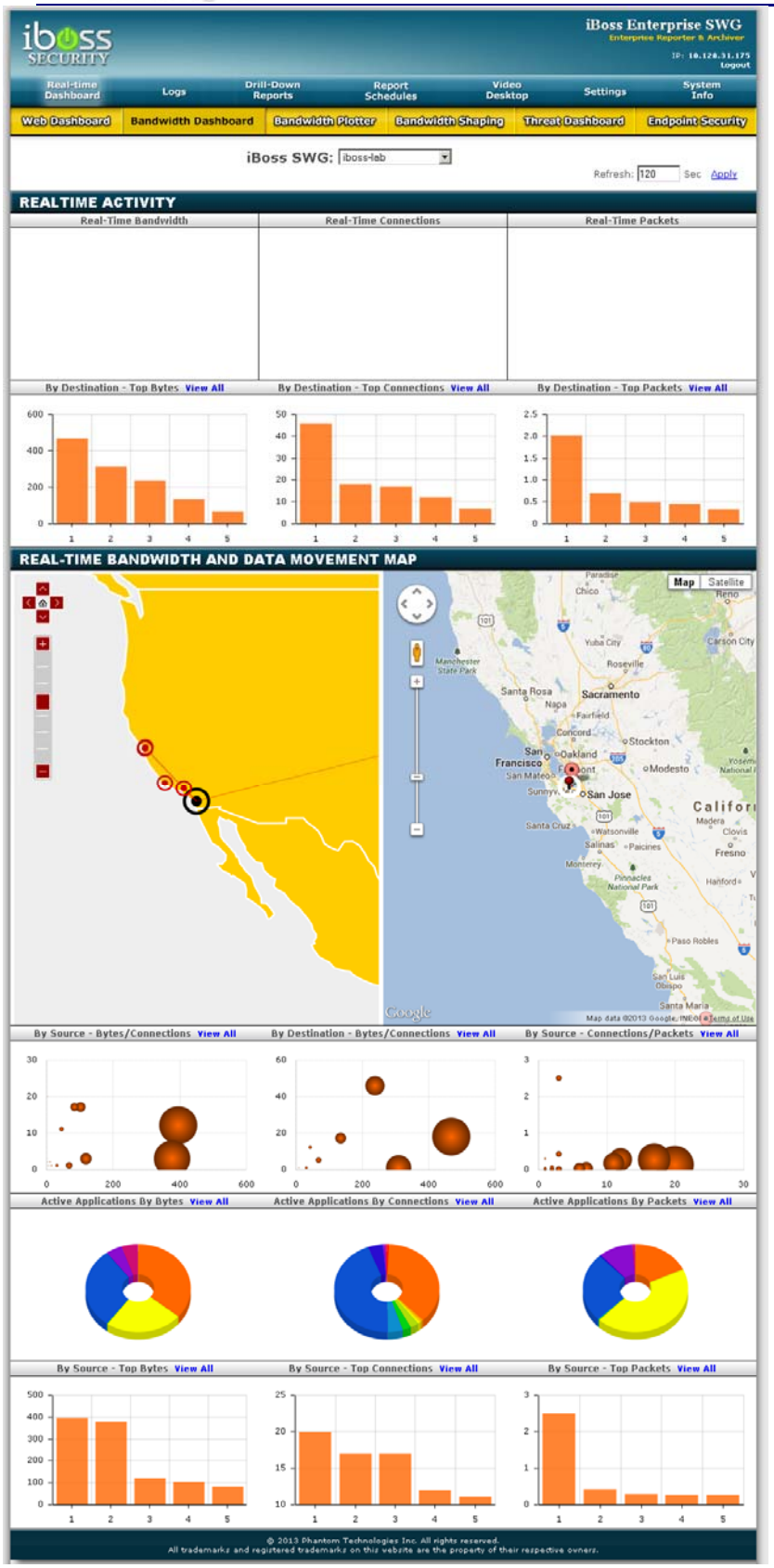

iBoss Enterprise SWG
Real-time Dashboard
Logs
Drill-Down Reports
Report Schedules
Video Desktop
Settings
System Info
Web Dashboard
Bandwidth Dashboard
Bandwidth Plotter
Bandwidth Shaping
Threat Dashboard
Endpoint Security
iBoss SWG:
Refresh:
Apply
REALTIME ACTIVITY
Real-Time Bandwidth
Real-Time Connections
Real-Time Packets
By Destination - Top Bytes View All
By Destination - Top Connections View All
By Destination - Top Packets View All
REAL-TIME BANDWIDTH AND DATA MOVEMENT MAP
By Source - Bytes/Connections View All
By Destination - Bytes/Connections View All
By Source - Connections/Packets View All
Active Applications By Bytes View All
Active Applications By Connections View All
Active Applications By Packets View All
By Source - Top Bytes View All
By Source - Top Connections View All
By Source - Top Packets View All

Figure 9 – Bandwidth Dashboard

1.4.1.2.1 *Real Time Activity*

This section has a series of graphs detailing the real time bandwidth activity. Hovering the mouse over the fields will yield additional information. The Real-Time Bandwidth and the Real-Time Connections are identical to the fields on the Web Dashboard. The three bar graphs all look at activity by destination. They list the top five by bytes, connections, and packets. In all three, clicking on the "View All" link yields a full list.

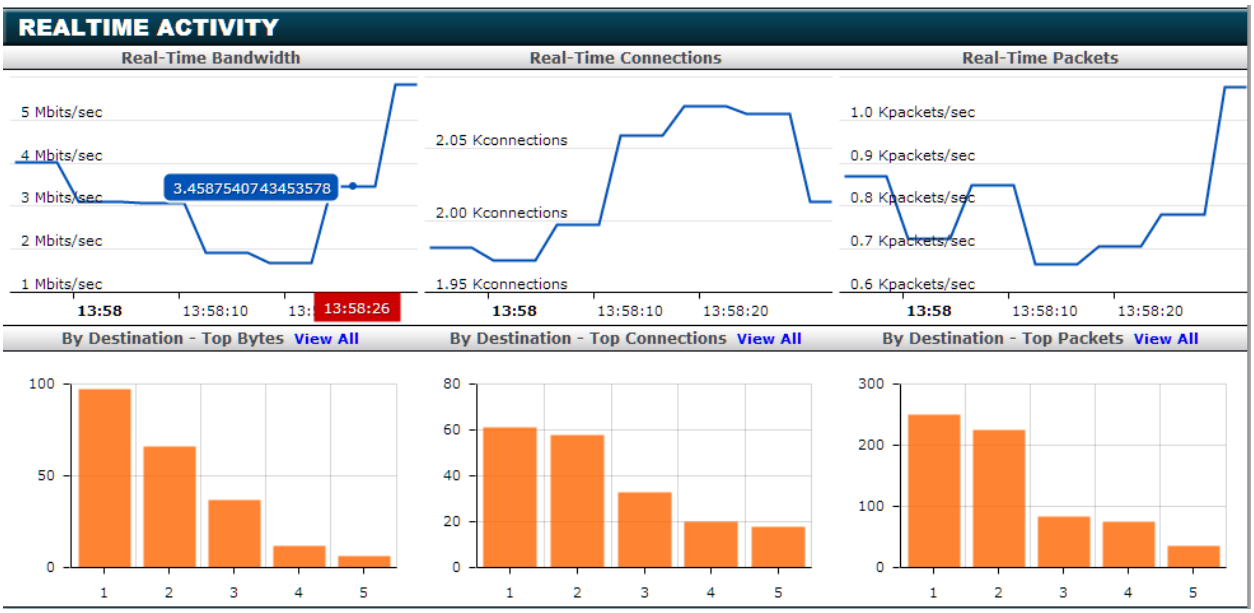


Figure 10 – Real Time Activity

1.4.1.2.2 *Data Movement Map*

This section has a pair of maps. The first map shows the data connections and is centered on the physical location of the filter. The second map focuses in on the physical location of the destination consuming the most bandwidth. Both maps can be moved and re-sized to show different locations.

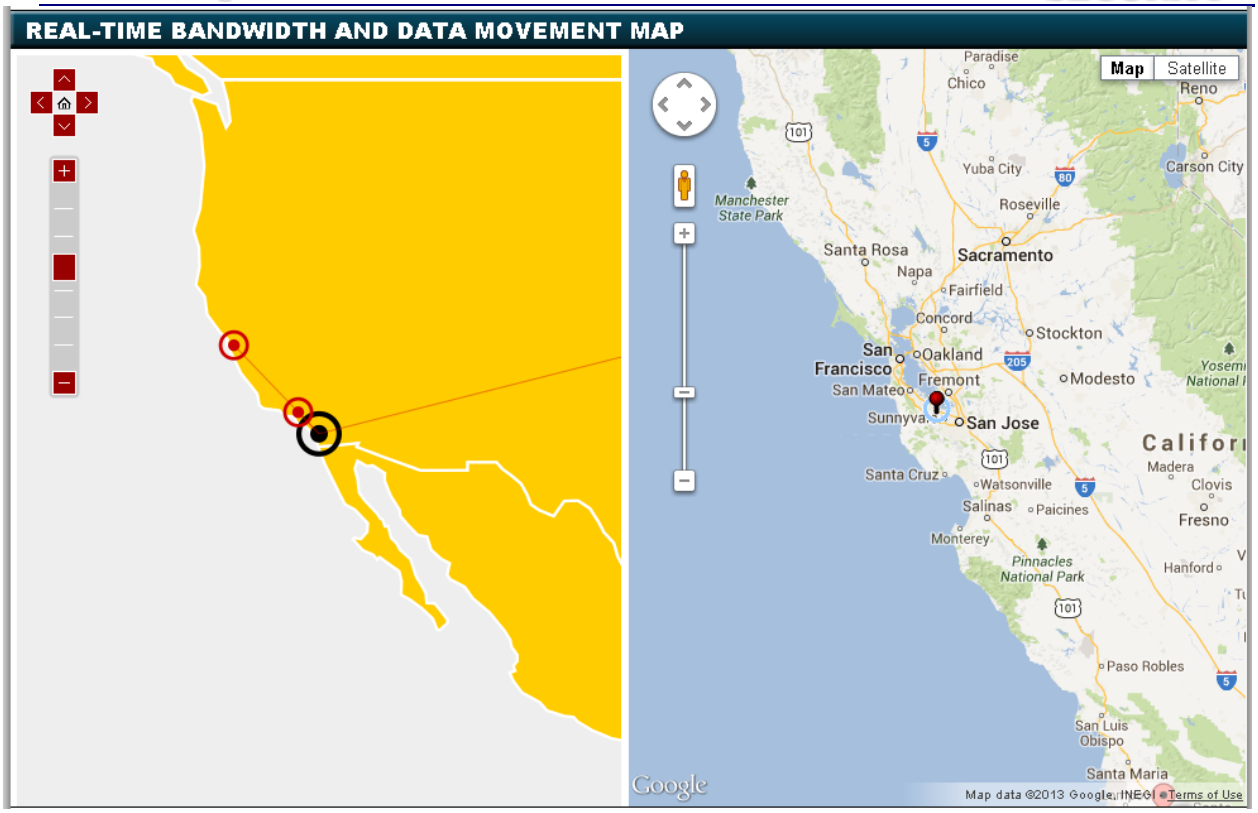


Figure 11 –Data Movement Maps

1.4.1.2.3 *Real-Time Bandwidth*

This section has a series of graphs detailing bandwidth activity from the perspective of the local hosts. Hovering the mouse over the fields yields more information. The first three fields offer a scatter plot with larger dots representing more bandwidth used. The second three have pie charts showing how the bandwidth is divided up. The last three show the top five sources as opposed to destination. They list the top five by bytes, connections, and packets. In all of them, clicking on the “View All” link yields a full list.

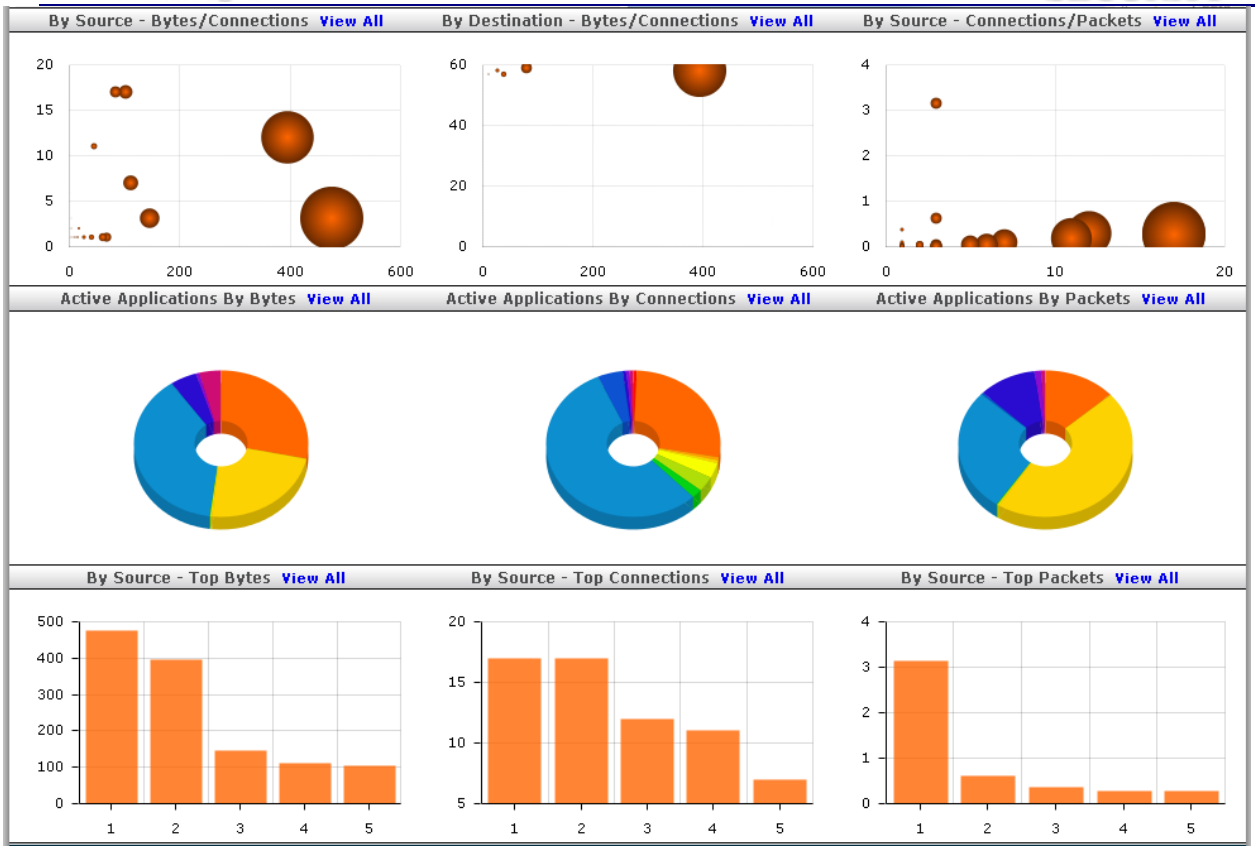

By Source - Bytes/Connections View All
By Destination - Bytes/Connections View All
By Source - Connections/Packets View All
Active Applications By Bytes View All
Active Applications By Connections View All
Active Applications By Packets View All
By Source - Top Bytes View All
By Source - Top Connections View All
By Source - Top Packets View All

Figure 12 – Real Time Bandwidth

1.4.1.3 Bandwidth Plotter

This section shows a single graph of kbytes/sec vs. number of connections. The larger 'dots' indicate more bandwidth being used by the sources identified. This graph, being much larger, gives a great deal more information. Hovering the mouse over the dots reveals details about the source.

Figure 13 – Real-Time Bandwidth Plotter

Clicking on one of the dots brings up details about all of the connections.

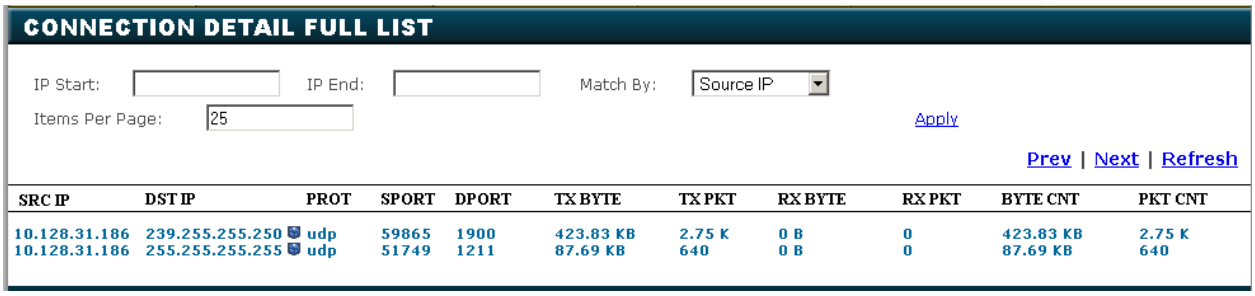

CONNECTION DETAIL FULL LIST
IP Start:
IP End:
Match By: Source IP
Items Per Page: 25
Apply
Prev | Next | Refresh
SRC IP DST IP PROT SPORT DPORT TX BYTE TX PKT RX BYTE RX PKT BYTE CNT PKT CNT
10.128.31.186 239.255.255.250 udp 59865 1900 423.83 KB 2.75 K 0 B 0 423.83 KB 2.75 K
10.128.31.186 255.255.255.255 udp 51749 1211 87.69 KB 640 0 B 0 87.69 KB 640

Figure 14 – Connection Detail Full List

1.4.1.4 Bandwidth Shaping

This page reveals information relating to the bandwidth shaping function of the iBoss SWG Web Filter.

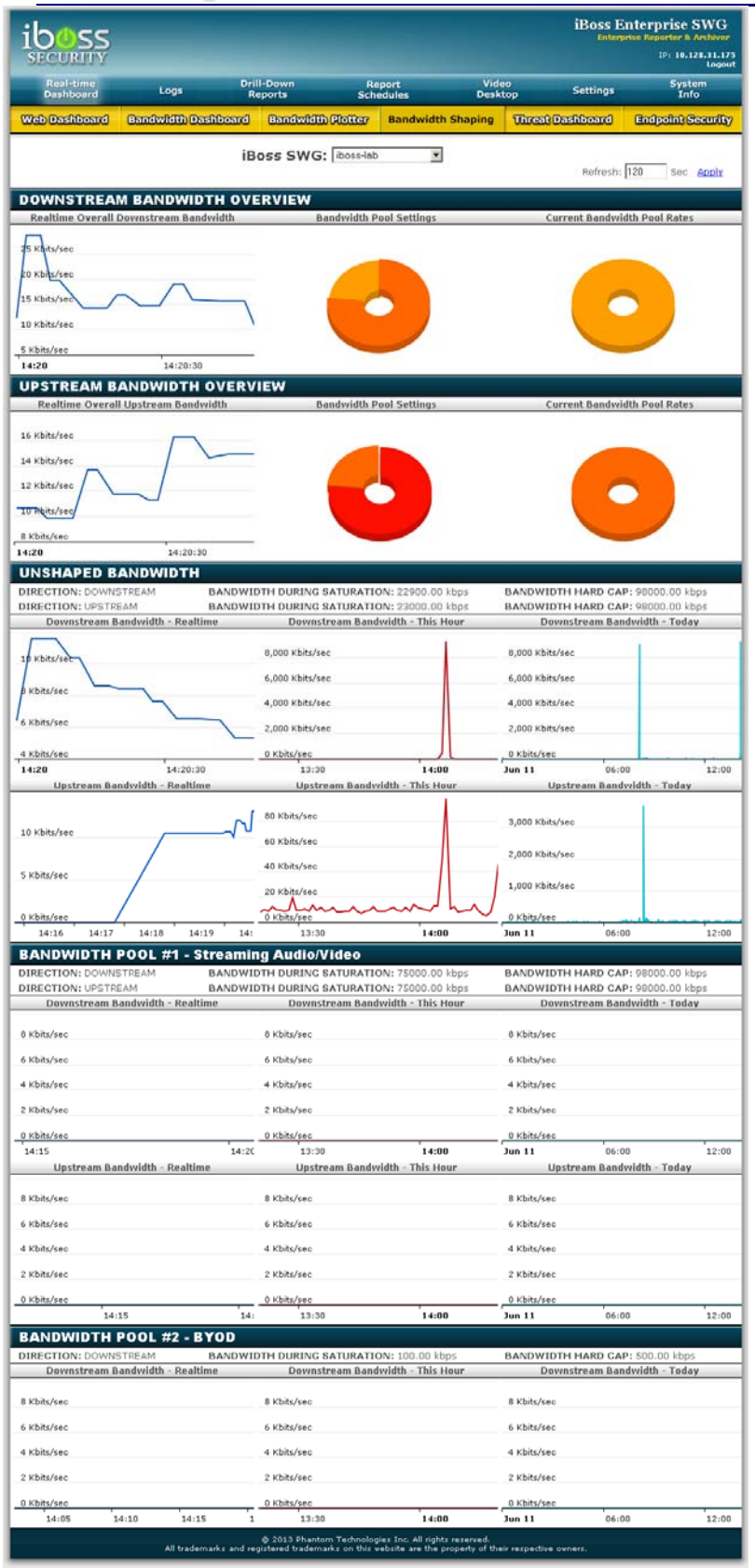

iboss SECURITY
iBoss Enterprise SWG
Enterprise Reporter & Archiver
IP: 10.128.31.175
Logout
Real-time Dashboard
Logs
Drill-Down Reports
Report Schedules
Video Desktop
Settings
System Info
Web Dashboard
Bandwidth Dashboard
Bandwidth Plotter
Bandwidth Shaping
Threat Dashboard
Endpoint Security
iBoss SWG: iboss-lab
Refresh: 120 Sec Apply
DOWNSTREAM BANDWIDTH OVERVIEW
Realtime Overall Downstream Bandwidth
Bandwidth Pool Settings
Current Bandwidth Pool Rates
UPSTREAM BANDWIDTH OVERVIEW
Realtime Overall Upstream Bandwidth
Bandwidth Pool Settings
Current Bandwidth Pool Rates
UNSHAPED BANDWIDTH
DIRECTION: DOWNSTREAM
BANDWIDTH DURING SATURATION: 22900.00 kbps
BANDWIDTH HARD CAP: 98000.00 kbps
DIRECTION: UPSTREAM
BANDWIDTH DURING SATURATION: 23000.00 kbps
BANDWIDTH HARD CAP: 98000.00 kbps
Downstream Bandwidth - Realtime
Downstream Bandwidth - This Hour
Downstream Bandwidth - Today
Upstream Bandwidth - Realtime
Upstream Bandwidth - This Hour
Upstream Bandwidth - Today
BANDWIDTH POOL #1 - Streaming Audio/Video
DIRECTION: DOWNSTREAM
BANDWIDTH DURING SATURATION: 75000.00 kbps
BANDWIDTH HARD CAP: 98000.00 kbps
DIRECTION: UPSTREAM
BANDWIDTH DURING SATURATION: 75000.00 kbps
BANDWIDTH HARD CAP: 98000.00 kbps
Downstream Bandwidth - Realtime
Downstream Bandwidth - This Hour
Downstream Bandwidth - Today
Upstream Bandwidth - Realtime
Upstream Bandwidth - This Hour
Upstream Bandwidth - Today
BANDWIDTH POOL #2 - BYOD
DIRECTION: DOWNSTREAM
BANDWIDTH DURING SATURATION: 100.00 kbps
BANDWIDTH HARD CAP: 500.00 kbps
Downstream Bandwidth - Realtime
Downstream Bandwidth - This Hour
Downstream Bandwidth - Today
© 2013 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 15 – Bandwidth Shaping

1.4.1.4.1 *Downstream Bandwidth Overview*

This section has three graphs all relating to downstream bandwidth. The first shows the overall downstream bandwidth. The second shows the bandwidth settings in pie chart form. The third shows a similar pie chart detailing how the bandwidth is actually used. The two charts share the same colors for easy comparison.

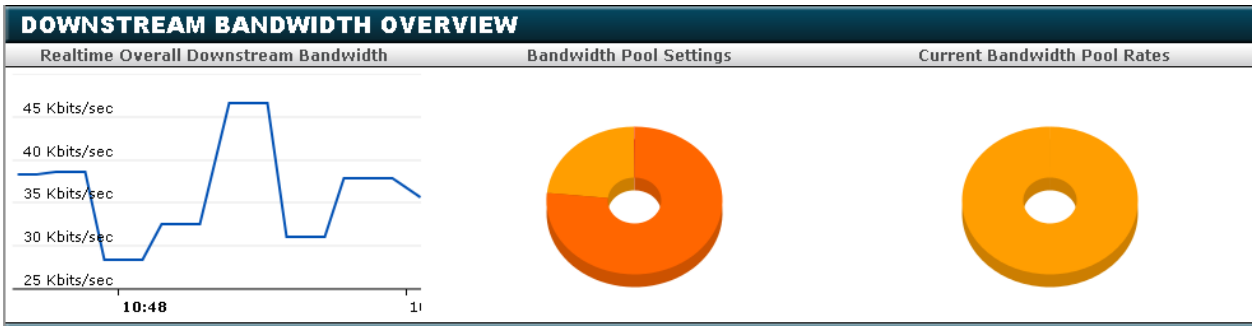


Figure 16 – Downstream Bandwidth Overview

1.4.1.4.2 *Upstream Bandwidth Overview*

This section has three graphs all relating to upstream bandwidth. The first shows the overall upstream bandwidth. The second shows the bandwidth settings in pie chart form. The third shows a similar pie chart detailing how the bandwidth is actually used. The two charts share the same colors for easy comparison.

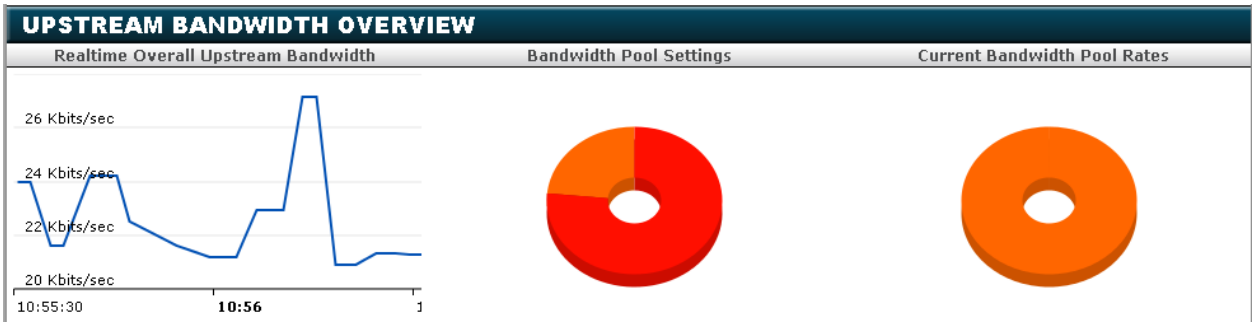


Figure 17 – Upstream Bandwidth Overview

1.4.1.4.3 *Unshaped Bandwidth*

This section has several graphs dedicated to revealing problems with bandwidth that is unshaped by the QoS rules. There are two sets of graphs. The first three are dedicated to Downstream Bandwidth. The second three are dedicated to Upstream Bandwidth. In both

cases, the first graph details the bandwidth in real time. The second details it over the past hour. The third details it over the past day.

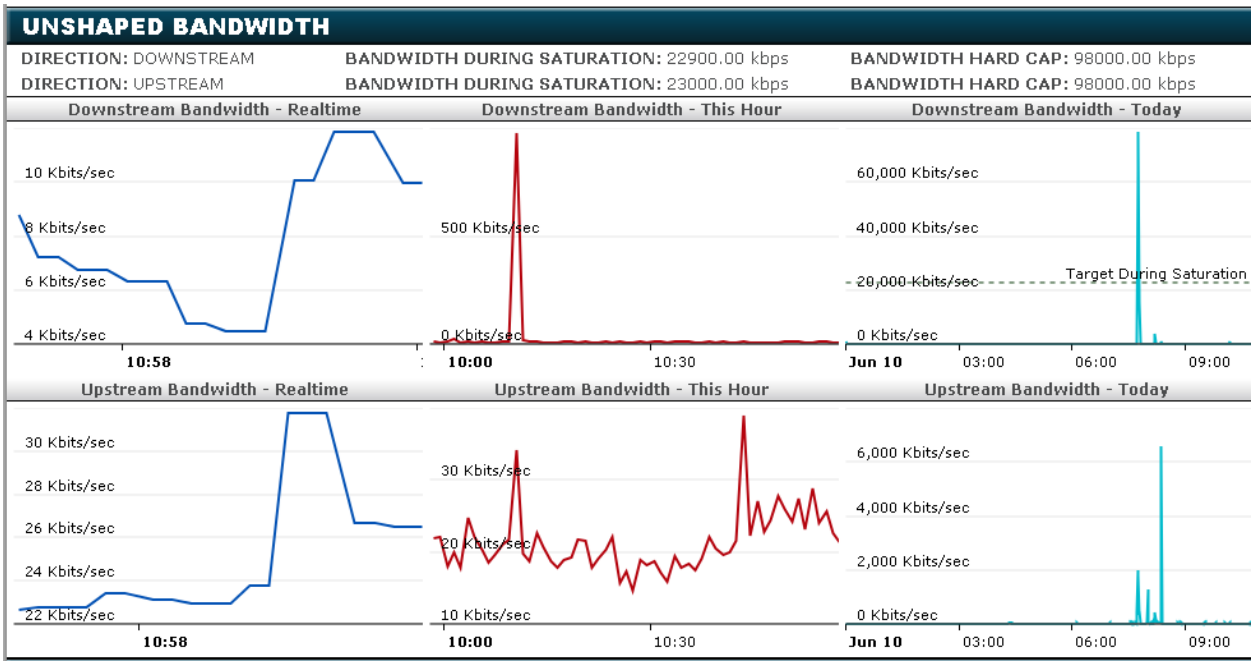


Figure 18 – Unshaped bandwidth

1.4.1.4.3.1 Bandwidth Pools

The last section on this page deals with the bandwidth pools as detailed in the iBoss SWG Web Filter. The number and shape of the pools will be determined by the number of pools and the rules assigned to them.

Similar to the way the Unshaped Bandwidth is displayed in figure 18, each pool, and the rules within each pool, are displayed as a series of graphs. These are Real Time, This Hour, and Today. In addition to the graphs, the bandwidth limits are displayed for easy reference.

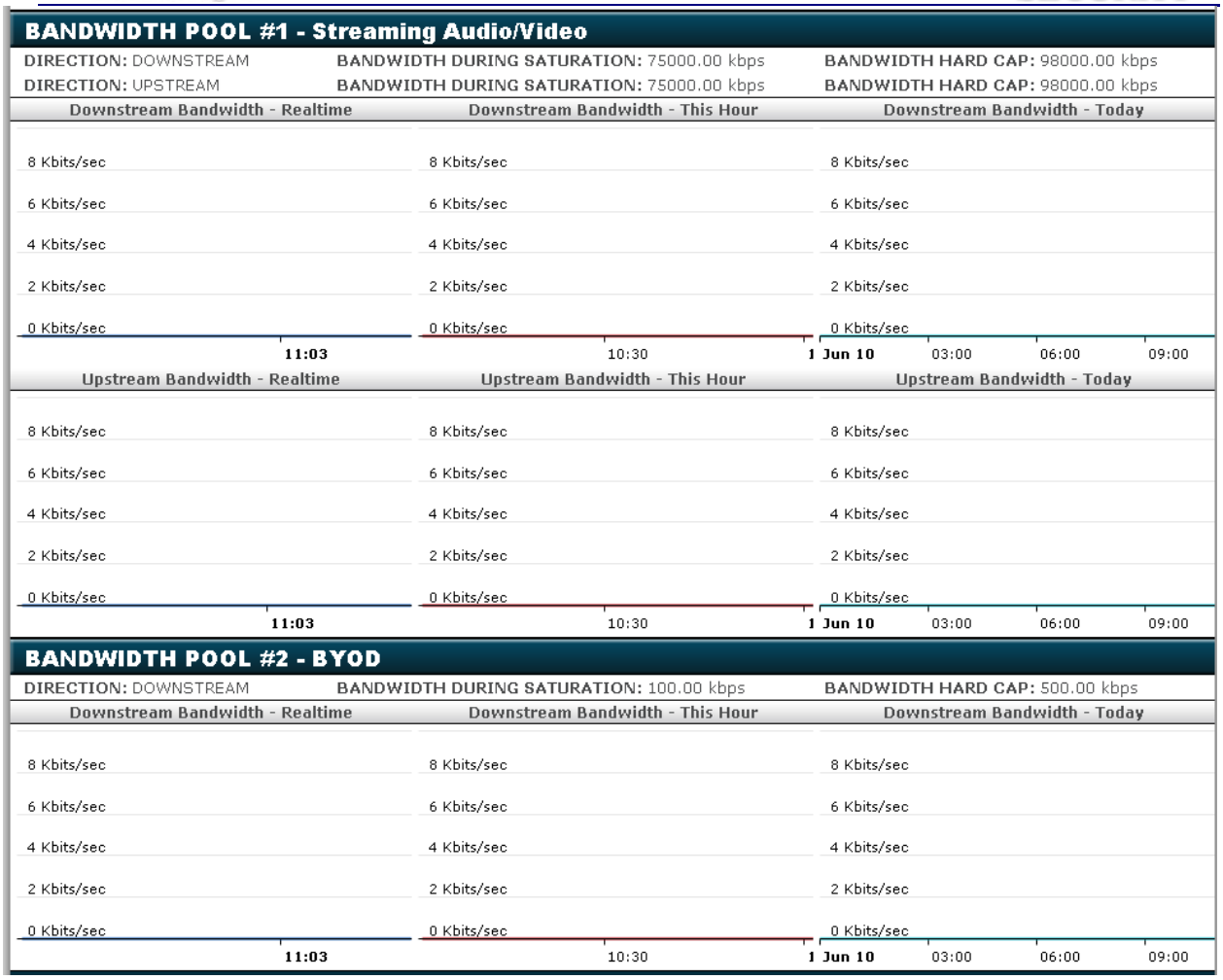


Figure 19 – Bandwidth Pools

1.4.1.5 Threat Dashboard

This page is only active if you have linked the Reporter to an iBoss Firewall with Intrusion Detection/Prevention. It allows you to see the threats detected by the ID/PS.

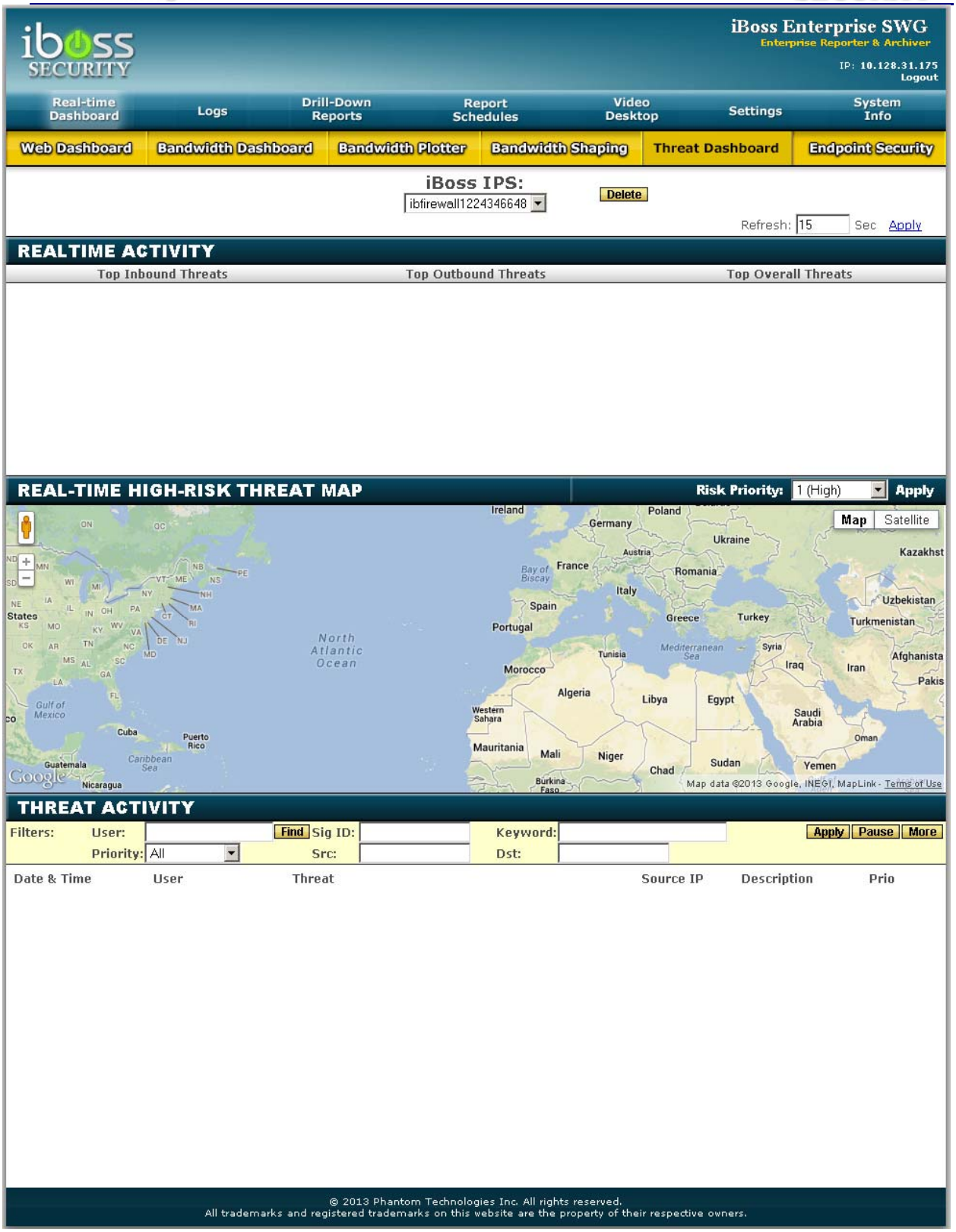


Figure 20 – Threat dashboard

1.4.1.5.1 *Real-Time Activity*

This section is a real time display of threats as they come in. It is divided into the top inbound threats, top outbound threats and top overall threats.

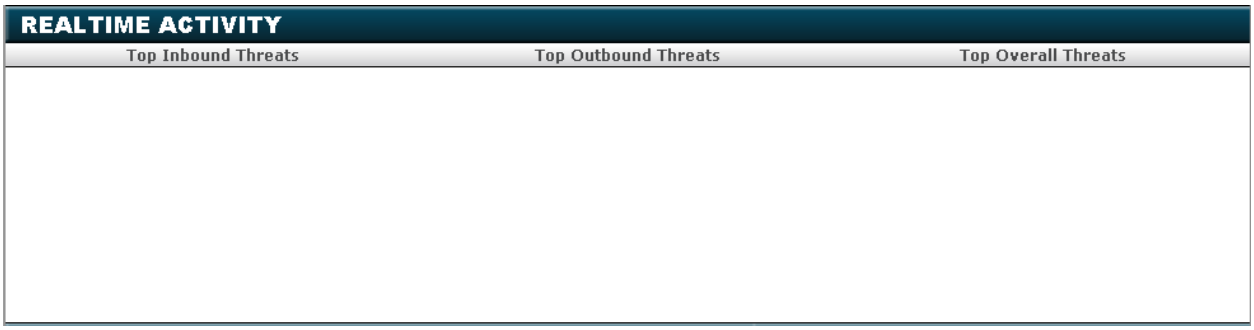


Figure 21 – Real-Time Activity

1.4.1.5.2 *Real Time High Risk Threat Map*

This section shows where the main threats to your network are coming from on the world map. There is a drop down menu at the top allowing you to display just the highest level threats down to the less severe threats.

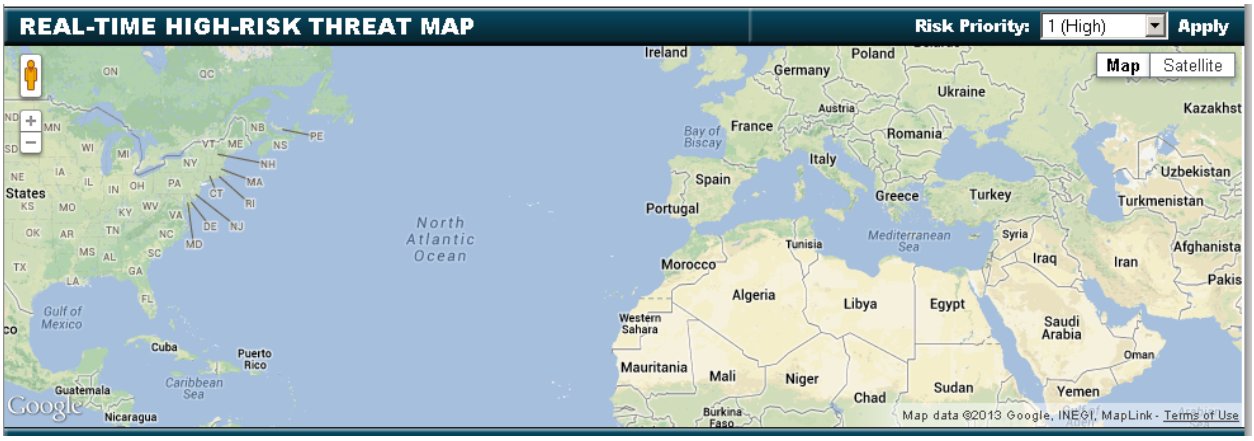


Figure 22 – Real Time High Risk Threat Map

1.4.1.5.3 *Threat Activity*

This section is a real time scrolling display of events as they occur. The list can be filtered to monitor for specific threats.

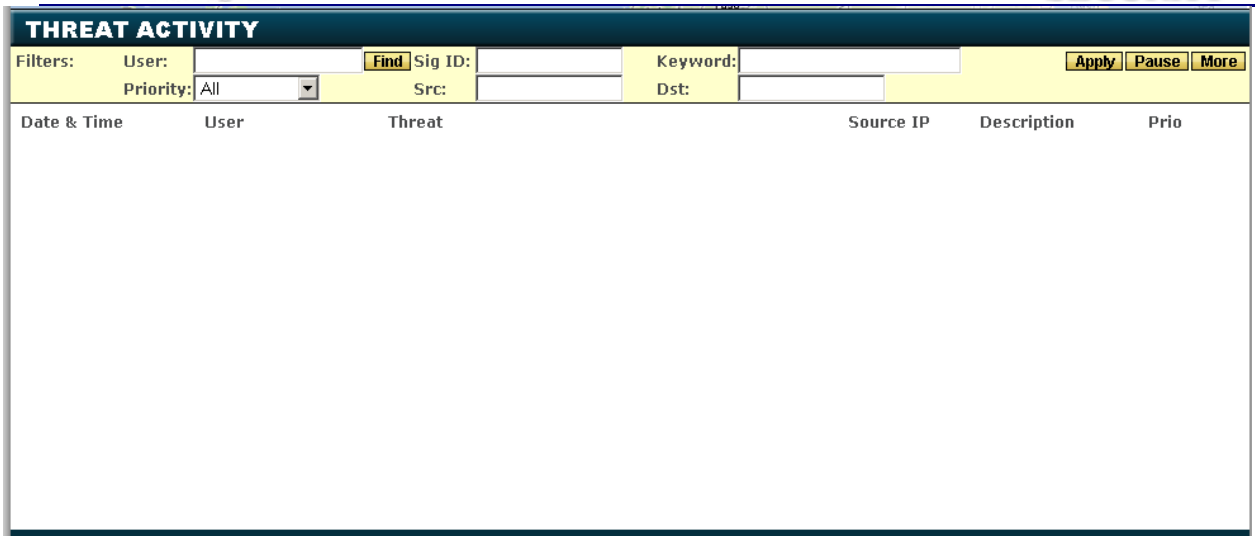


Figure 22 – Threat Activity

1.4.1.6 Endpoint Security

This section displays information about the iBoss Endpoint Security system. Please refer to the iBoss Endpoint Security guide for more details about these features.

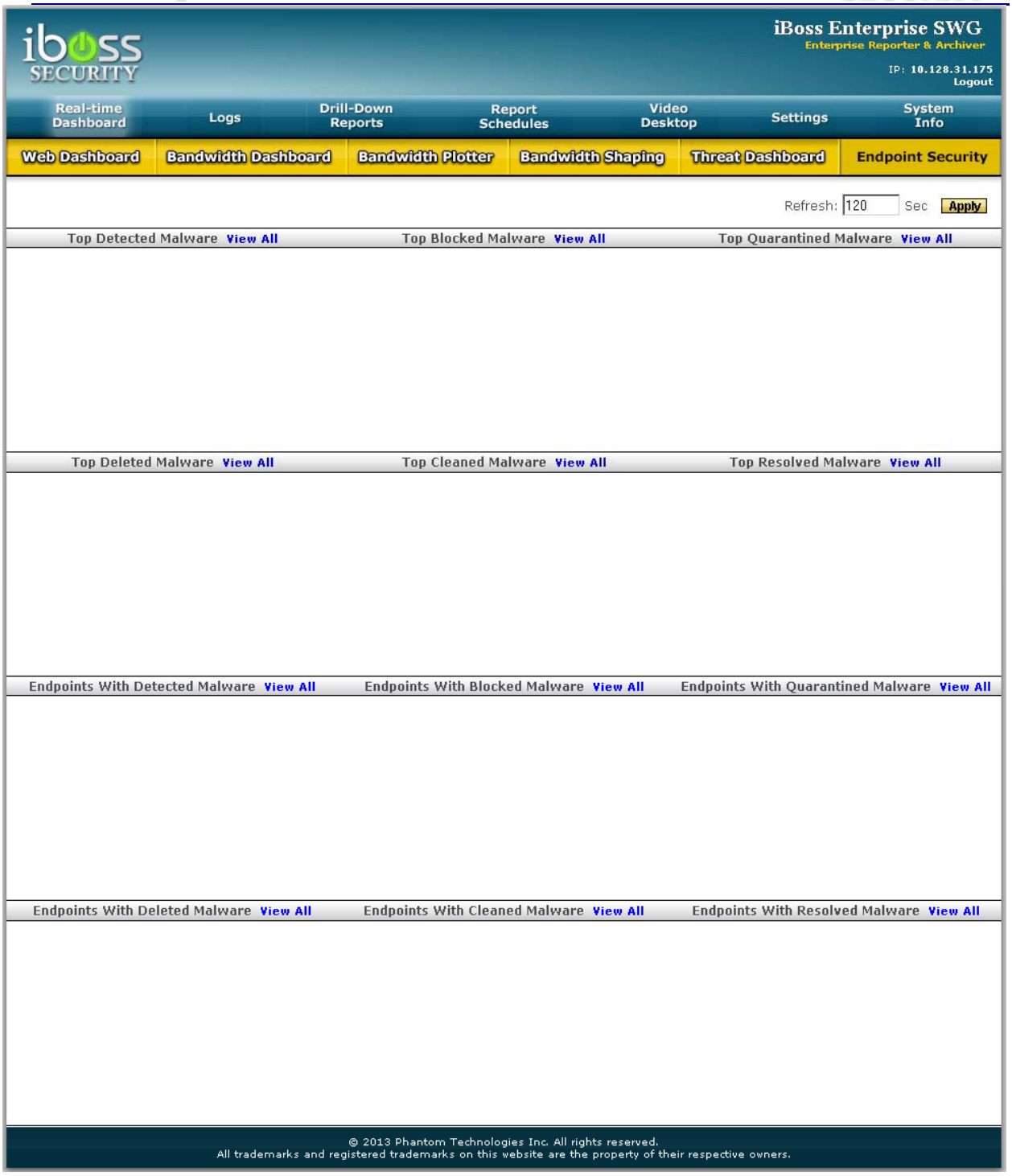


Figure 23 – Endpoint Security

1.4.2 Logs

This section allows you to view the logs of activity. There are two sections. The first is for web activity. The second is for threat activity.

1.4.2.1 Web

This section displays the logs of web activity from the iBoss Web Filters that are connected to the unit.

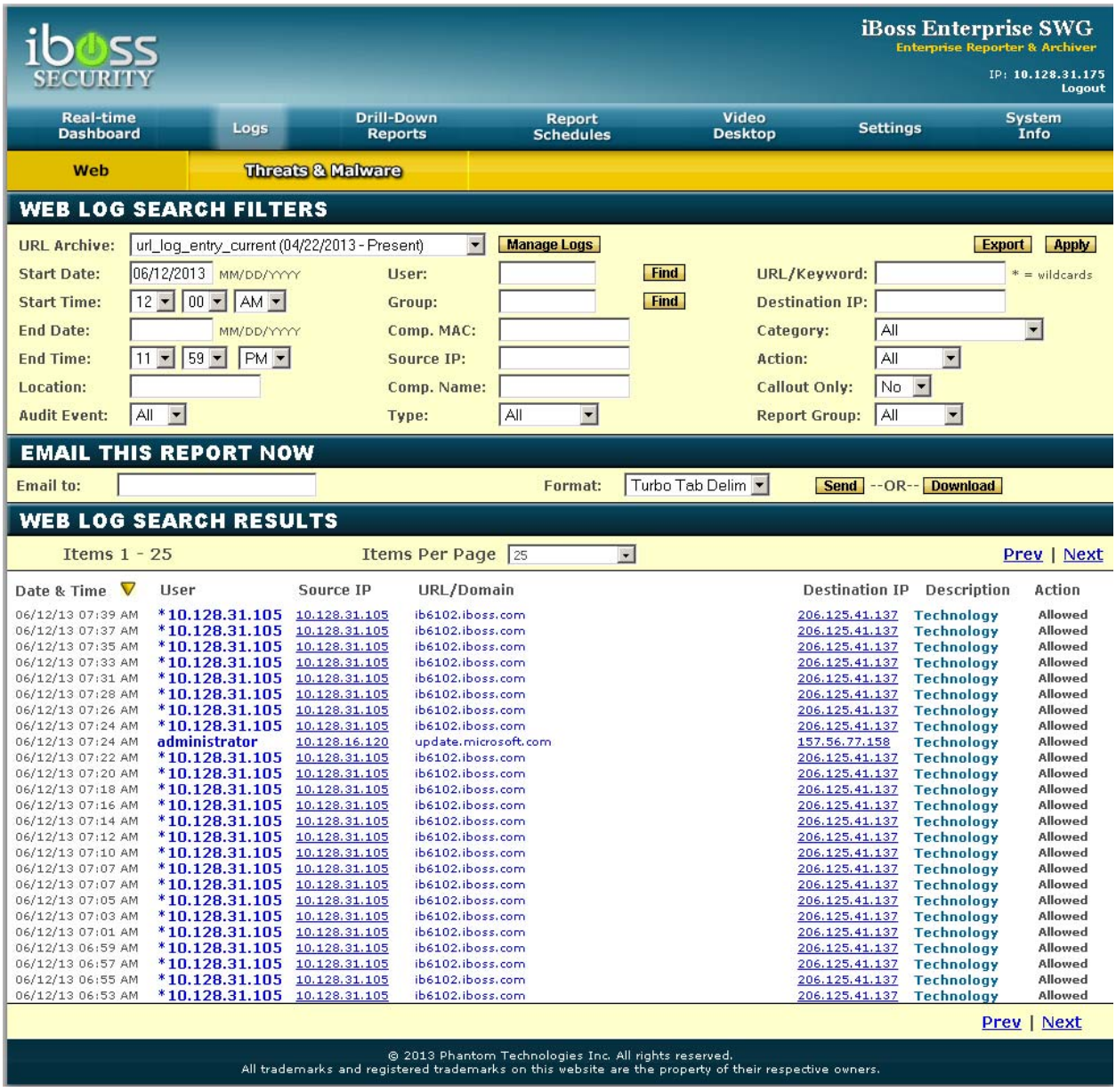

iboss SECURITY
iBoss Enterprise SWG
Enterprise Reporter & Archiver
IP: 10.128.31.175
Logout
Real-time Dashboard
Logs
Drill-Down Reports
Report Schedules
Video Desktop
Settings
System Info
Web
Threats & Malware
WEB LOG SEARCH FILTERS
URL Archive: url_log_entry_current (04/22/2013 - Present)
Manage Logs
Export
Apply
Start Date: 06/12/2013 MM/DD/YYYY
User:
Find
URL/Keyword:
* = wildcards
Start Time: 12 00 AM
Group:
Find
Destination IP:
End Date: MM/DD/YYYY
Comp. MAC:
Category: All
End Time: 11 59 PM
Source IP:
Action: All
Location:
Comp. Name:
Callout Only: No
Audit Event: All
Type: All
Report Group: All
EMAIL THIS REPORT NOW
Email to:
Format: Turbo Tab Delim
Send --OR-- Download
WEB LOG SEARCH RESULTS
Items 1 - 25
Items Per Page 25
Prev | Next
Date & Time
User
Source IP
URL/Domain
Destination IP
Description
Action
06/12/13 07:39 AM *10.128.31.105 10.128.31.105 ib6102.iboss.com 206.125.41.137 Technology Allowed
06/12/13 07:37 AM *10.128.31.105 10.128.31.105 ib6102.iboss.com 206.125.41.137 Technology Allowed
06/12/13 07:35 AM *10.128.31.105 10.128.31.105 ib6102.iboss.com 206.125.41.137 Technology Allowed
06/12/13 07:33 AM *10.128.31.105 10.128.31.105 ib6102.iboss.com 206.125.41.137 Technology Allowed
06/12/13 07:31 AM *10.128.31.105 10.128.31.105 ib6102.iboss.com 206.125.41.137 Technology Allowed
06/12/13 07:28 AM *10.128.31.105 10.128.31.105 ib6102.iboss.com 206.125.41.137 Technology Allowed
06/12/13 07:26 AM *10.128.31.105 10.128.31.105 ib6102.iboss.com 206.125.41.137 Technology Allowed
06/12/13 07:24 AM *10.128.31.105 10.128.31.105 ib6102.iboss.com 206.125.41.137 Technology Allowed
06/12/13 07:24 AM administrator 10.128.16.120 update.microsoft.com 157.56.77.158 Technology Allowed
06/12/13 07:22 AM *10.128.31.105 10.128.31.105 ib6102.iboss.com 206.125.41.137 Technology Allowed
06/12/13 07:20 AM *10.128.31.105 10.128.31.105 ib6102.iboss.com 206.125.41.137 Technology Allowed
06/12/13 07:18 AM *10.128.31.105 10.128.31.105 ib6102.iboss.com 206.125.41.137 Technology Allowed
06/12/13 07:16 AM *10.128.31.105 10.128.31.105 ib6102.iboss.com 206.125.41.137 Technology Allowed
06/12/13 07:14 AM *10.128.31.105 10.128.31.105 ib6102.iboss.com 206.125.41.137 Technology Allowed
06/12/13 07:12 AM *10.128.31.105 10.128.31.105 ib6102.iboss.com 206.125.41.137 Technology Allowed
06/12/13 07:10 AM *10.128.31.105 10.128.31.105 ib6102.iboss.com 206.125.41.137 Technology Allowed
06/12/13 07:07 AM *10.128.31.105 10.128.31.105 ib6102.iboss.com 206.125.41.137 Technology Allowed
06/12/13 07:07 AM *10.128.31.105 10.128.31.105 ib6102.iboss.com 206.125.41.137 Technology Allowed
06/12/13 07:05 AM *10.128.31.105 10.128.31.105 ib6102.iboss.com 206.125.41.137 Technology Allowed
06/12/13 07:03 AM *10.128.31.105 10.128.31.105 ib6102.iboss.com 206.125.41.137 Technology Allowed
06/12/13 07:01 AM *10.128.31.105 10.128.31.105 ib6102.iboss.com 206.125.41.137 Technology Allowed
06/12/13 06:59 AM *10.128.31.105 10.128.31.105 ib6102.iboss.com 206.125.41.137 Technology Allowed
06/12/13 06:57 AM *10.128.31.105 10.128.31.105 ib6102.iboss.com 206.125.41.137 Technology Allowed
06/12/13 06:55 AM *10.128.31.105 10.128.31.105 ib6102.iboss.com 206.125.41.137 Technology Allowed
06/12/13 06:53 AM *10.128.31.105 10.128.31.105 ib6102.iboss.com 206.125.41.137 Technology Allowed
Prev | Next
© 2013 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 24 – Web Logs

1.4.2.1.1 *Web Log Search Filters*

This section contains the filter controls that mold the results displayed below. These filters allow hiding other URLs and only showing results you'd like to see. This makes it easier to diagnose and look through the URLs. You can search for date ranges, users, groups, Mac

addresses, source IP addresses, computer names, URL or keyword filter, location, category, action and callout. Once you have made these filters, click the "**Apply**" button above the search filters. You can export this. You may also send this report directly from this page by entering email information under the section for Email This Report Now and clicking the "**Send**" button. You may also generate a report schedule by clicking on the "**Create Report Schedule**" button.

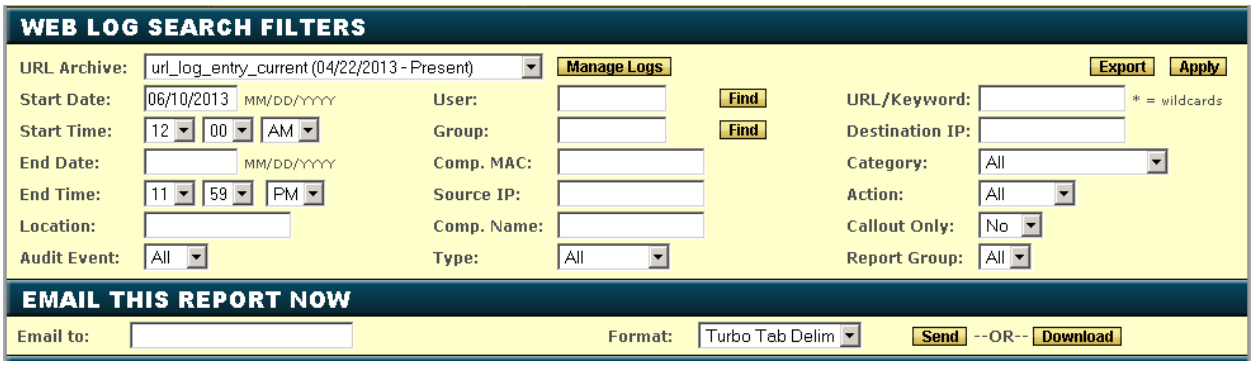


Figure 25 – Web Log Search Filters

1.4.2.1.2 *Site Callouts*

These are callouts in which site logos are displayed and search terms are tagged. For example, sites like Google will show the logo of Google and the term that was used to search with.

06/10/13 01:13 PM khit 10.128.16.119 www.google.com/gen_204?v=3&s=web&action=&ei=VTO2UYij... 216.239.32.20 Search Engin.. Allowed
06/10/13 01:13 PM khit 10.128.16.119 www.google.com/gen_204?atyp=i&ct=phandle&cad=1,0,det... 216.239.32.20 Search Engin.. Allowed
06/10/13 01:13 PM khit 10.128.16.119 www.google.com/xjs/_/js/k=xjs.s.en_US.h6ozd5YZptc.O/... 216.239.32.20 Search Engin.. Allowed
06/10/13 01:13 PM (khit) 10.128.16.119 www.google.com/search?safe=active&sclient=psy-ab&q=w... 216.239.32.20 Search E.. Allowed
Google
Google search: 'web+filter'
View
06/10/13 01:13 PM khit 10.128.16.119 www.google.com/gen_204?atyp=i&ct=1&cad=1&rsm=6&ei=VD... 216.239.32.20 Search Engin.. Allowed
06/10/13 01:13 PM khit 10.128.16.119 ssl.gstatic.com 74.125.239.111 Bandwidth 94 B
06/10/13 01:13 PM khit 10.128.16.119 www.google.com/s?gs_rn=16&gs_ri=psy-ab&suggest=p&cp=... 216.239.32.20 Search Engin.. Allowed
06/10/13 01:13 PM khit 10.128.16.119 www.google.com/s?gs_rn=16&gs_ri=psy-ab&suggest=p&cp=... 216.239.32.20 Search Engin.. Allowed
06/10/13 01:13 PM khit 10.128.16.119 nosslsearch.google.com 216.239.32.20 Bandwidth 4.79 KB
06/10/13 01:13 PM khit 10.128.16.119 ssl.gstatic.com 74.125.239.111 Bandwidth 239 B
06/10/13 01:13 PM khit 10.128.16.119 www.google.com/gen_204?v=3&s=web&action=&ei=VDO2UZLa... 216.239.32.20 Search Engin.. Allowed
06/10/13 01:13 PM khit 10.128.16.119 www.google.com/xjs/_/js/k=xjs.s.en_US.h6ozd5YZptc.O/... 216.239.32.20 Search Engin.. Allowed

Figure 26 - Site Callouts

1.4.2.2 Threats & Malware

This section displays the log files from the IPS units that are attached to the reporter. It displays the results in reverse chronological order.

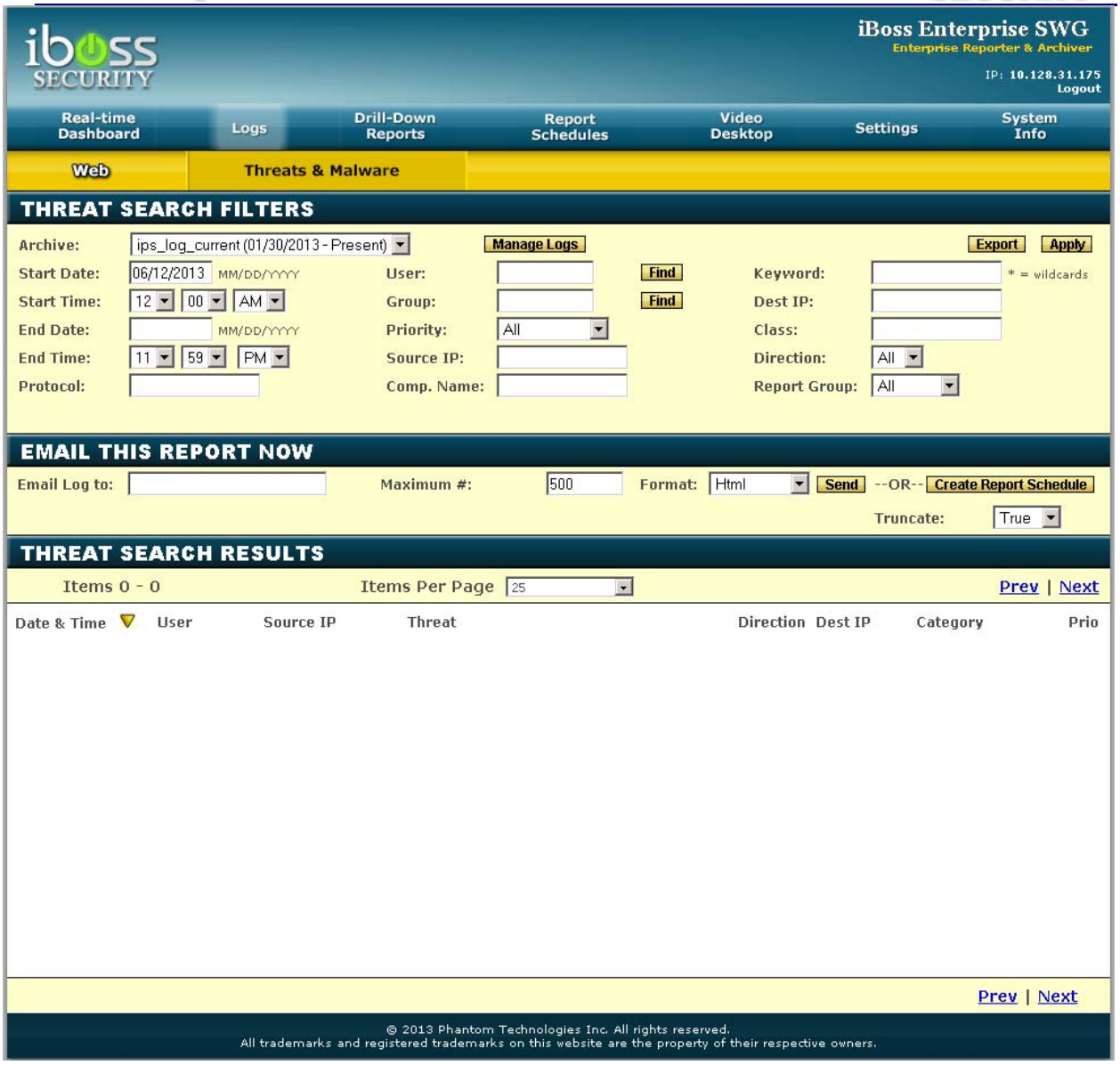


Figure 27 – Threats & Malware

1.4.2.2.1 *Threat Search Filters*

This section contains the filter controls that mold the results displayed below. These filters allow hiding threats and only showing filters in which you'd like to see. This makes it easier to diagnose and look through the threats. You can search for date ranges, users, groups, Mac addresses, source IP addresses, computer names, protocol, keyword filter, location or class. Once you have made these filters, click the "**Apply**" button above the search filters. You can export this. You may also send this report directly from this page by entering email information under the section for Email This Report Now and clicking the "**Send**" button. You may also generate a report schedule by clicking on the "**Create Report Schedule**" button.

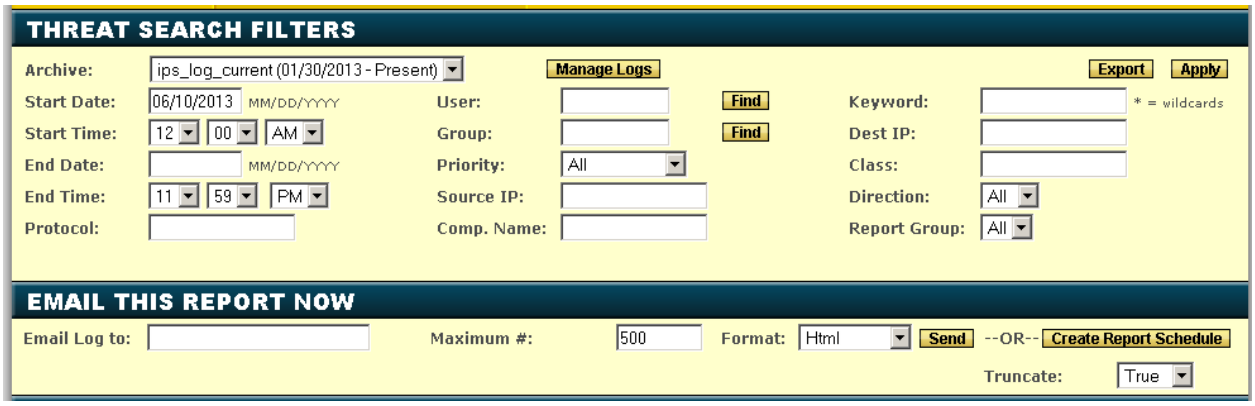


Figure 28 – Threat Search Filters

1.4.3 Drop-Down Reports

This section allows you to view the generated reports that exist within the report manager. You can generate and delete reports within this section. In addition, this is where you access individual reports for viewing. The generated reports page contains a breakdown of the auto-generated daily reports as well as the user generated reports. There is also a drop down menu allowing you to display reports that only pertain to certain reporting groups.

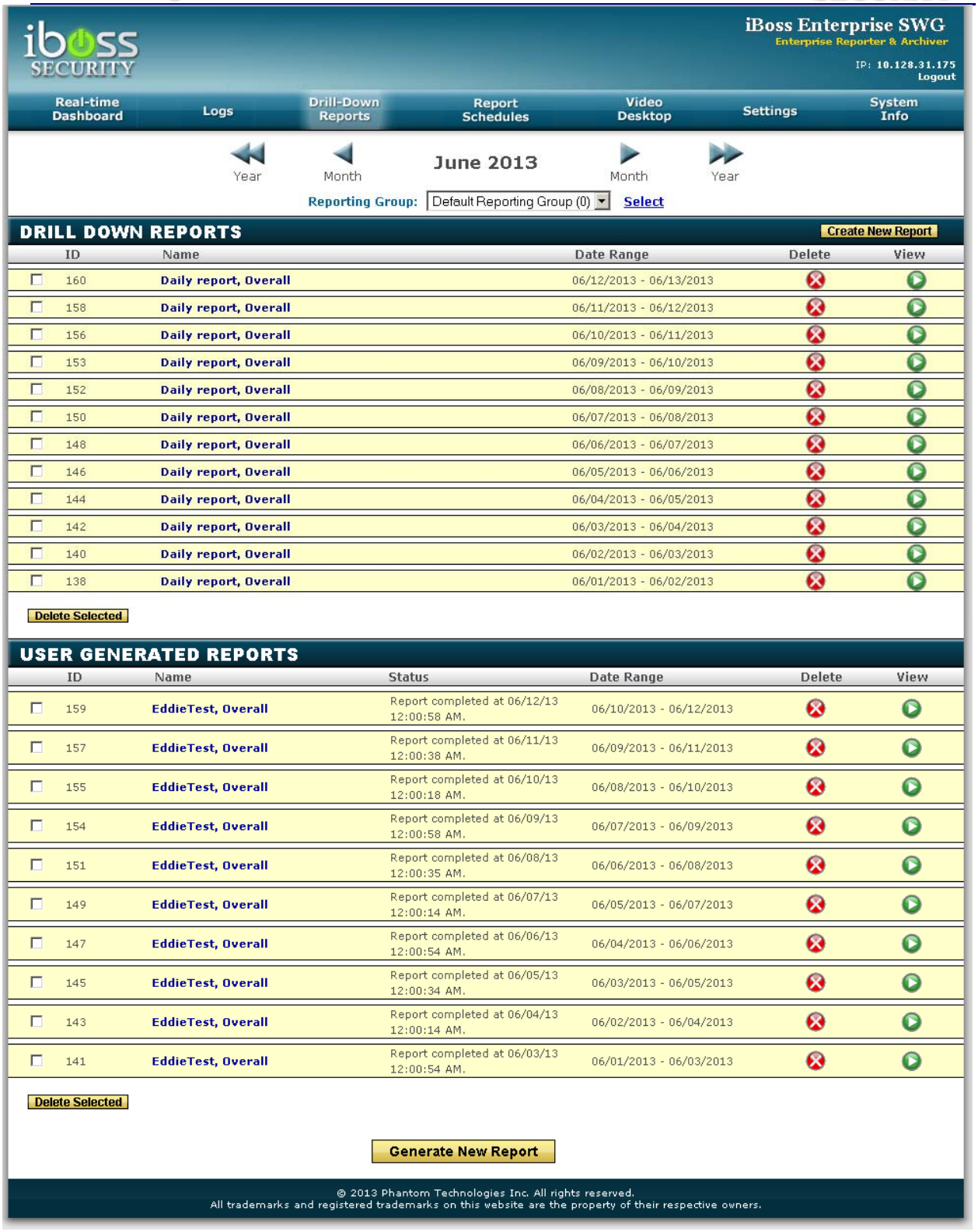

iboss SECURITY
iBoss Enterprise SWG
Enterprise Reporter & Archiver
IP: 10.128.31.175
Logout
Real-time Dashboard
Logs
Drill-Down Reports
Report Schedules
Video Desktop
Settings
System Info
Year
Month
June 2013
Month
Year
Reporting Group: Default Reporting Group (0) Select
DRILL DOWN REPORTS
Create New Report
ID Name Date Range Delete View
160 Daily report, Overall 06/12/2013 - 06/13/2013
158 Daily report, Overall 06/11/2013 - 06/12/2013
156 Daily report, Overall 06/10/2013 - 06/11/2013
153 Daily report, Overall 06/09/2013 - 06/10/2013
152 Daily report, Overall 06/08/2013 - 06/09/2013
150 Daily report, Overall 06/07/2013 - 06/08/2013
148 Daily report, Overall 06/06/2013 - 06/07/2013
146 Daily report, Overall 06/05/2013 - 06/06/2013
144 Daily report, Overall 06/04/2013 - 06/05/2013
142 Daily report, Overall 06/03/2013 - 06/04/2013
140 Daily report, Overall 06/02/2013 - 06/03/2013
138 Daily report, Overall 06/01/2013 - 06/02/2013
Delete Selected
USER GENERATED REPORTS
ID Name Status Date Range Delete View
159 EddieTest, Overall Report completed at 06/12/13 12:00:58 AM. 06/10/2013 - 06/12/2013
157 EddieTest, Overall Report completed at 06/11/13 12:00:38 AM. 06/09/2013 - 06/11/2013
155 EddieTest, Overall Report completed at 06/10/13 12:00:18 AM. 06/08/2013 - 06/10/2013
154 EddieTest, Overall Report completed at 06/09/13 12:00:58 AM. 06/07/2013 - 06/09/2013
151 EddieTest, Overall Report completed at 06/08/13 12:00:35 AM. 06/06/2013 - 06/08/2013
149 EddieTest, Overall Report completed at 06/07/13 12:00:14 AM. 06/05/2013 - 06/07/2013
147 EddieTest, Overall Report completed at 06/06/13 12:00:54 AM. 06/04/2013 - 06/06/2013
145 EddieTest, Overall Report completed at 06/05/13 12:00:34 AM. 06/03/2013 - 06/05/2013
143 EddieTest, Overall Report completed at 06/04/13 12:00:14 AM. 06/02/2013 - 06/04/2013
141 EddieTest, Overall Report completed at 06/03/13 12:00:54 AM. 06/01/2013 - 06/03/2013
Delete Selected
Generate New Report
© 2013 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 29 – Drop-Down Reports

1.4.3.1 Report Types

Generated reports come in two basic types, auto-generated daily reports and user generated reports. Auto-generated daily reports are automatically created by the iBoss. There is one daily report generated per day that includes statistics for usage on that day. User generated reports are reports that are created by the user. These reports can contain custom date ranges, include particular groups, and include only certain statistics among other things.

1.4.3.2 Deleting Reports

Reports are deleted as space becomes necessary, but you can select and delete any report on this page by clicking on the “Delete” button next to the report or selecting the checkboxes of the reports you wish to delete and clicking on the “Delete Selected” button. Please note that deleting reports may take a while to process as the iBoss will clean out all related data pertaining to the report.

1.4.3.3 Exporting PDF Reports

To export a report, click on the QuickPDF button when viewing the report. This will generate a PDF Report which you can select which options to include in the report.

1.4.3.4 Generating a Report

To generate a report, click on the “Generate New Report” button toward the bottom of the list of generated reports. This will lead to a page that presents the options available when creating a report. There are many options available that can be configured when generating a report such as the included group users, the types of statistics you would like to include in the report, as well as the date range for the report.

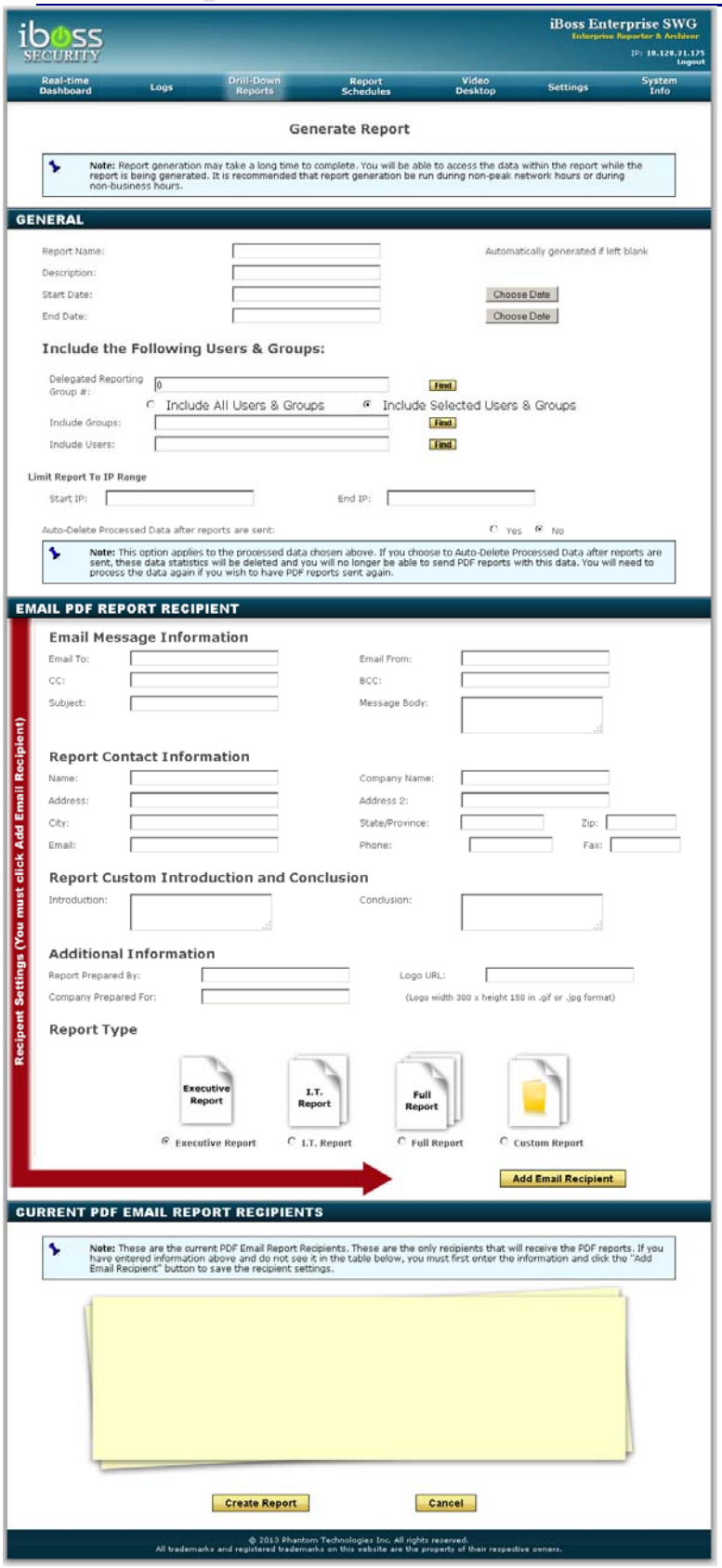

iboss SECURITY
iBoss Enterprise SWG
Enterprise Reporter & Archiver
IP: 10.120.31.175
Logout
Real-time Dashboard
Logs
Drill-Down Reports
Report Schedules
Video Desktop
Settings
System Info
Generate Report
Note: Report generation may take a long time to complete. You will be able to access the data within the report while the report is being generated. It is recommended that report generation be run during non-peak network hours or during non-business hours.
GENERAL
Report Name:
Automatically generated if left blank
Description:
Start Date:
Choose Date
End Date:
Choose Date
Include the Following Users & Groups:
Delegated Reporting Group #:
Find
Include All Users & Groups
Include Selected Users & Groups
Include Groups:
Find
Include Users:
Find
Limit Report To IP Range
Start IP:
End IP:
Auto-Delete Processed Data after reports are sent:
Yes
No
Note: This option applies to the processed data chosen above. If you choose to Auto-Delete Processed Data after reports are sent, these data statistics will be deleted and you will no longer be able to send PDF reports with this data. You will need to process the data again if you wish to have PDF reports sent again.
EMAIL PDF REPORT RECIPIENT
Recipient Settings (You must click Add Email Recipient)
Email Message Information
Email To:
Email From:
CC:
BCC:
Subject:
Message Body:
Report Contact Information
Name:
Company Name:
Address:
Address 2:
City:
State/Province:
Zip:
Email:
Phone:
Fax:
Report Custom Introduction and Conclusion
Introduction:
Conclusion:
Additional Information
Report Prepared By:
Logo URL:
Company Prepared For:
(Logo width 300 x height 150 in .gif or .jpg format)
Report Type
Executive Report
I.T. Report
Full Report
Executive Report
I.T. Report
Full Report
Custom Report
Add Email Recipient
CURRENT PDF EMAIL REPORT RECIPIENTS
Note: These are the current PDF Email Report Recipients. These are the only recipients that will receive the PDF reports. If you have entered information above and do not see it in the table below, you must first enter the information and click the "Add Email Recipient" button to save the recipient settings.
Create Report
Cancel
© 2013 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 30 - Generate Report

1.4.3.4.1 *General Report Settings*

This section contains the general settings for the report to be generated. Below is a description of the options:

Report Name	This is the friendly name for the report.
Description	This allows you to enter a description for the report.
Start Date	This is the date from which to start including data for this report. All report statistics within this report will be based on this start date.
End Date	This is the end date which you wish to stop including data for the report. The end date is not included in the statistics for this report. All data up to this end date is included. The end date must be after the start date.
Include the Following Users and Groups:	
Delegated Reporting Group #	This allows you to limit the data in the report to the specified reporting group number. Otherwise the entire set of data is used.
Include All Users & Groups / Include Selected Users & Groups	Selecting *Include Selected Users & Groups* enables the next two fields. If *Include All Users & Groups* is selected, the data in the next two fields is irrelevant, and all data is used regardless of user or group.
Include Groups	Groups to be included in the report. Multiple groups can be included.
Include Users	Users to be included in the report. Multiple users can be included.
Limit Report to IP Range	If used, all data in the report has to have a local IP address between the start and end IP addresses put in.

1.4.3.4.2 *Email PDF Report Recipient*

This section allows the report to be emailed once generation is complete. Since report generation may take a while to complete, you may choose to configure these settings so that an email can be sent once the email generation process is complete to avoid having to wait for the report to complete.

1.4.3.4.2.1 Email Message Information

Enter the email information including the recipient, sender, cc, bcc, subject, and message body. This will send the email to another person which looks like it comes from you with a personalized message.

1.4.3.4.2.2 Report Contact Information

This information shows up on the cover page of the Emailed PDF Report. Enter the Name, Company Name, Address, City, State, Zip, Email, Phone and Fax.

1.4.3.4.2.3 Report Custom Introduction and Conclusion

This information shows up on the second page for the introduction and the last page which is the conclusion. Enter a custom introduction and a custom conclusion.

1.4.3.4.2.4 Additional Information

This information shows who the report was prepared by, add a logo, and who it was prepared for. This allows you to customize the report to show that you were the one who prepared it and who it was prepared for. The Logo URL allows you to add a link to an image (.gif or .jpg) to the cover page of the iBoss Report.

1.4.3.4.2.5 Report Type

This allows you to choose which type of report to send. There are four options to choose from: Executive, I.T., Full, and Custom. The Executive report has the least information in the report but is used for a quick overview. The I.T. Report show more information such as IP statistics, Port statistics, Application Statistics, and Bandwidth statistics. The Full Report shows all of the contained data. The Custom Report allows you to choose which you may choose which options to include in the report.

You may also choose to have the report automatically deleted once it is emailed. Please note that email reports only provide a high level summary of the report. If you would like to keep the report so that you can access the details and all of the drill down capability, do not select this option.

Note: You must have a configured SMTP server for the email setting to work. This is configured through “Settings” tab of the report manager.

1.4.3.4.3 *Creating the Report*

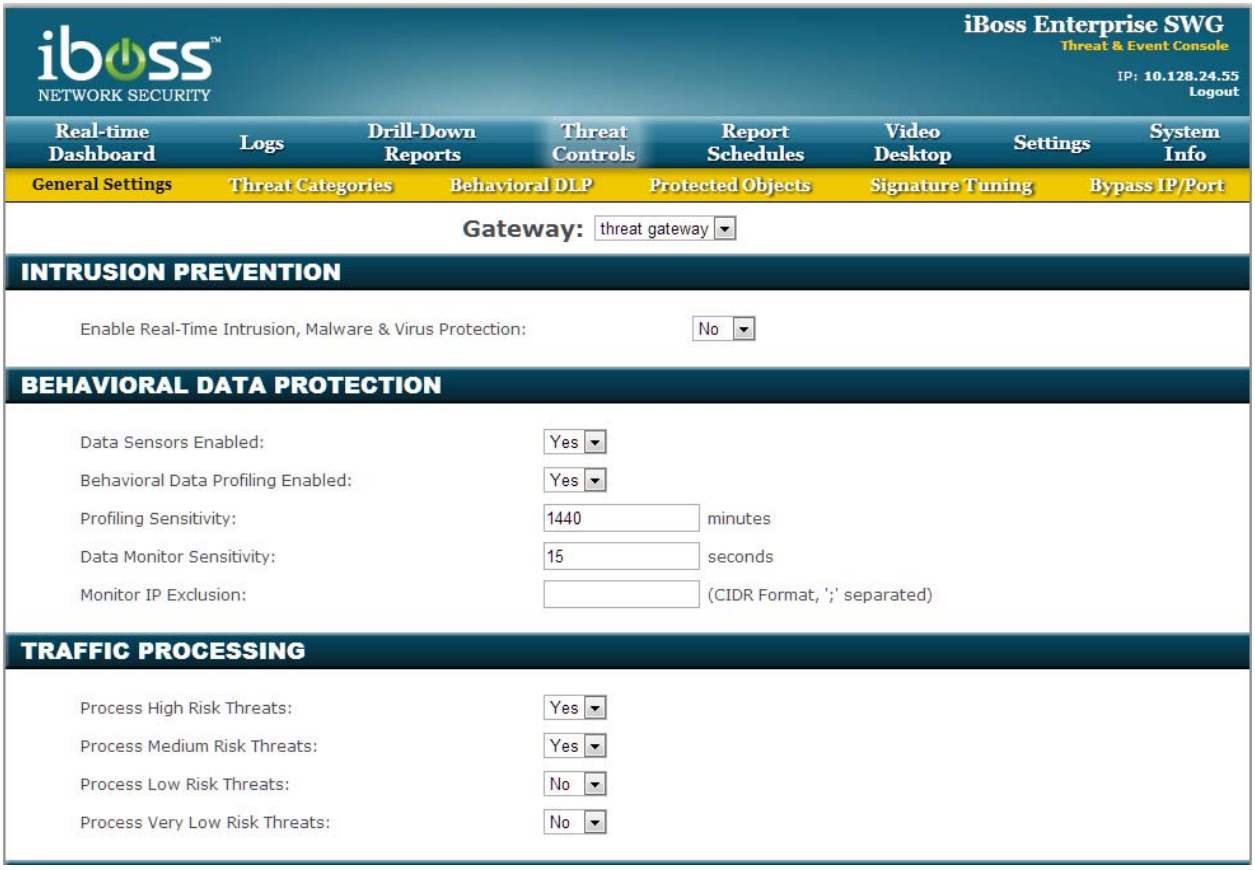
Once you have configured these options, click on the “Create Report” button on the bottom of the page. This will trigger the generation of the report and take you back to the Generated Report screen. Please note that only one report generation can occur simultaneously. If there is another report generation in progress, this report will be queued and scheduled for generation.

You can view the status of the report generation by refreshing the generated reports page. To do this, click on the Generated Reports button on the top of that page. You can access the report while it is being generated, however the data will continue to change as more data is added to the report until the report generation process is complete. If the report includes the current day, statistics will continue to accumulate until the report complete at which point no more data for the current day will be added to the report.

1.4.4 Threat Controls

This section defines controls the iboss IPS systems attached to this reporter. More details can be found in the IPS manual.

1.4.4.1 General Settings



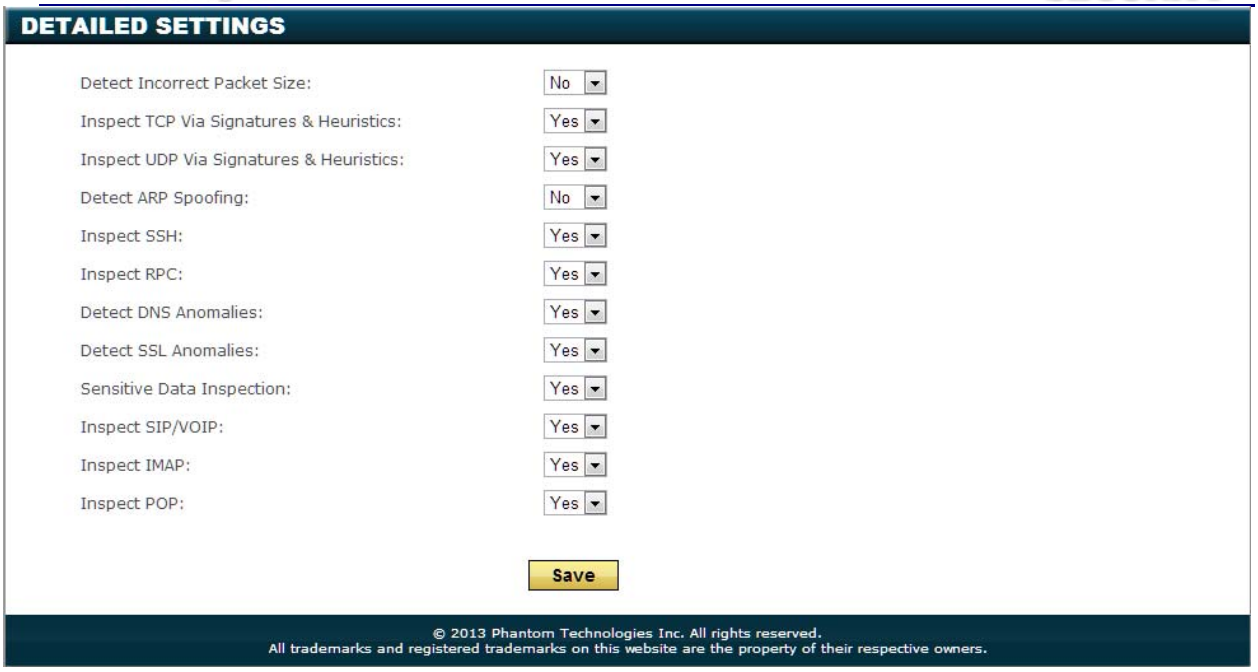
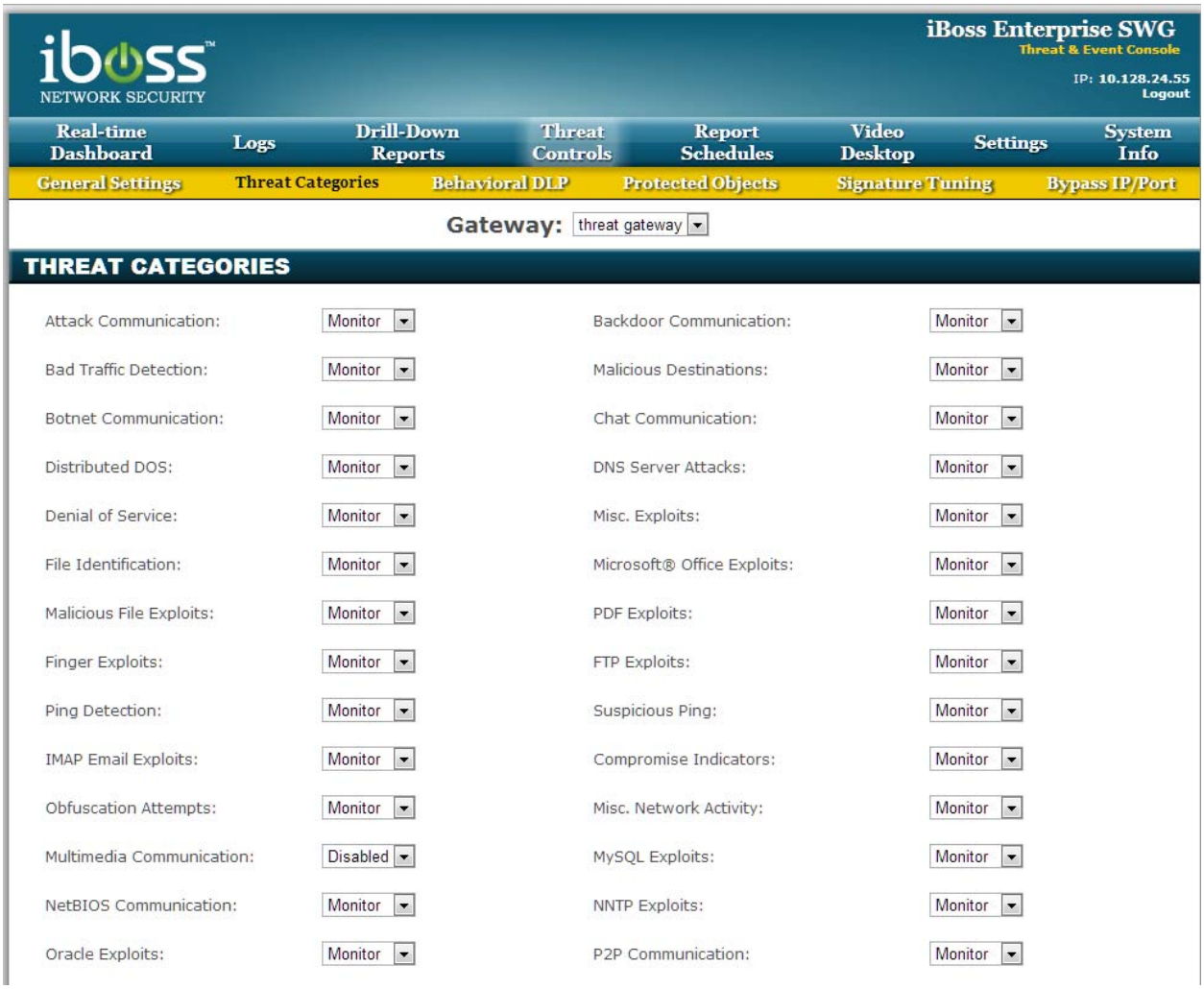

DETAILED SETTINGS
Detect Incorrect Packet Size: No
Inspect TCP Via Signatures & Heuristics: Yes
Inspect UDP Via Signatures & Heuristics: Yes
Detect ARP Spoofing: No
Inspect SSH: Yes
Inspect RPC: Yes
Detect DNS Anomalies: Yes
Detect SSL Anomalies: Yes
Sensitive Data Inspection: Yes
Inspect SIP/VOIP: Yes
Inspect IMAP: Yes
Inspect POP: Yes
Save
© 2013 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 31 – General Settings

1.4.4.2 Threat Categories



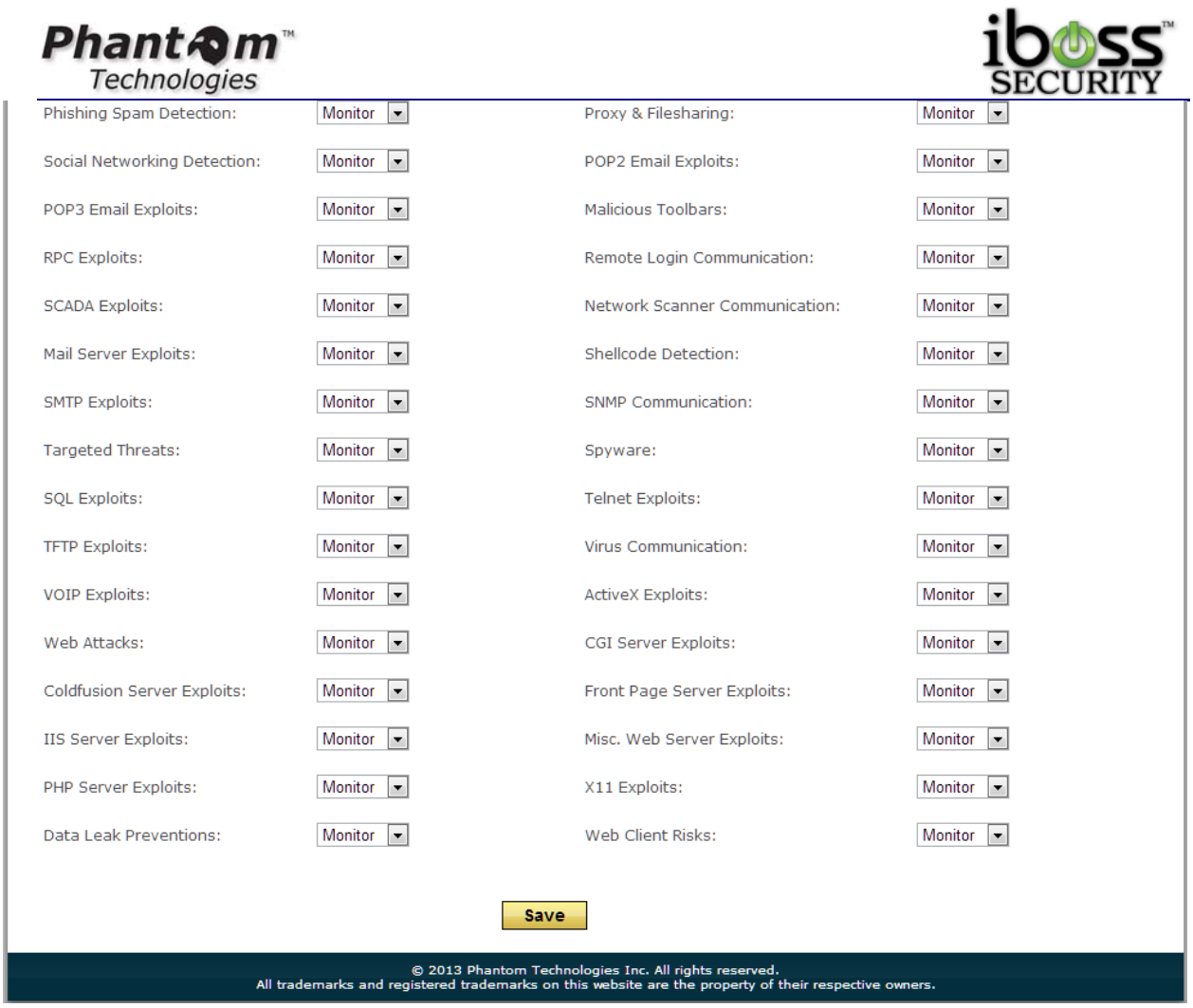


Figure 32 – Threat Categories

1.4.4.3 Behavioral DLP

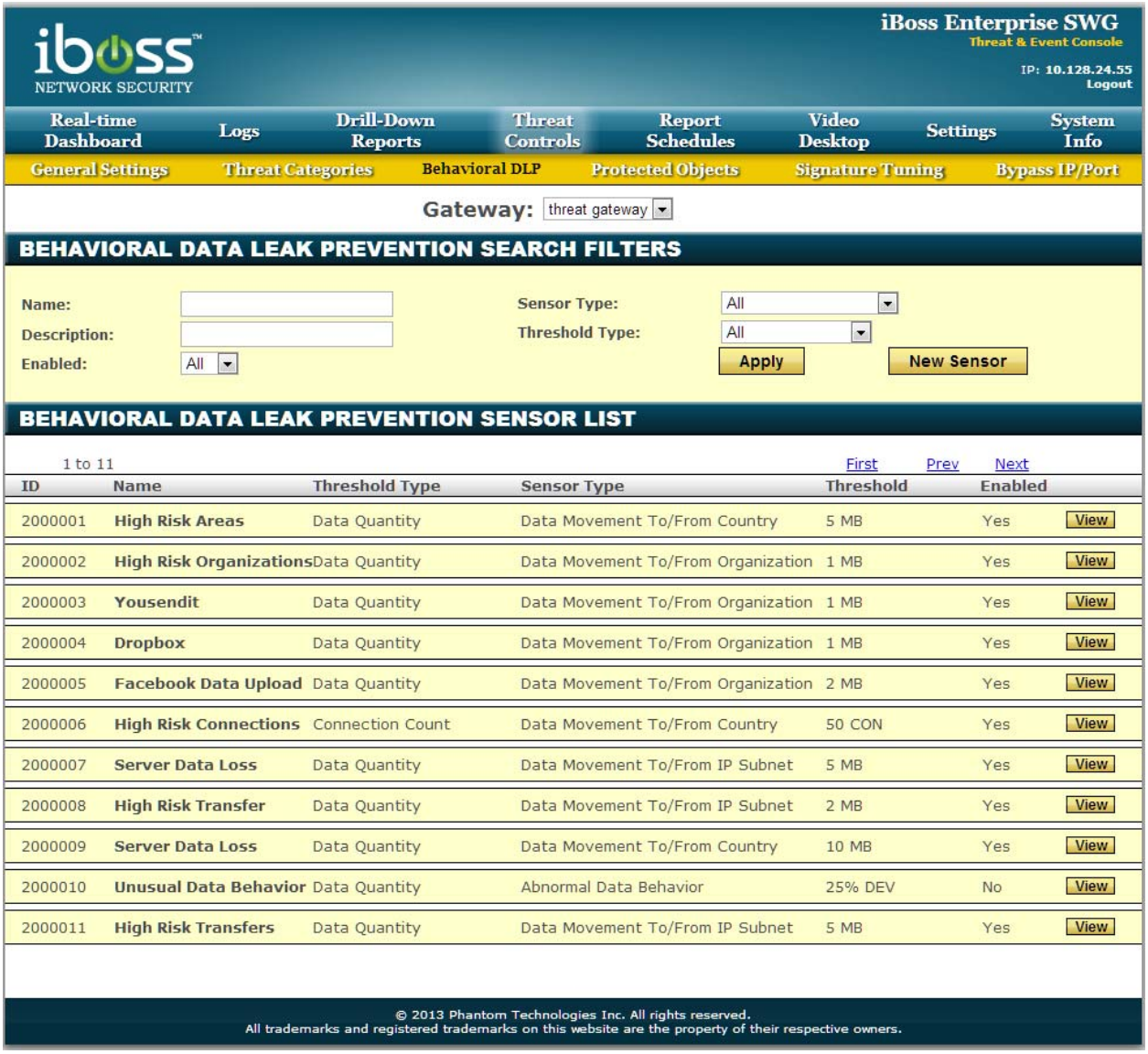

iboss NETWORK SECURITY
iBoss Enterprise SWG
Threat & Event Console
IP: 10.128.24.55
Logout
Real-time Dashboard
Logs
Drill-Down Reports
Threat Controls
Report Schedules
Video Desktop
Settings
System Info
General Settings
Threat Categories
Behavioral DLP
Protected Objects
Signature Tuning
Bypass IP/Port
Gateway: threat gateway
BEHAVIORAL DATA LEAK PREVENTION SEARCH FILTERS
Name:
Description:
Enabled: All
Sensor Type: All
Threshold Type: All
Apply
New Sensor
BEHAVIORAL DATA LEAK PREVENTION SENSOR LIST
1 to 11
First Prev Next
ID Name Threshold Type Sensor Type Threshold Enabled
2000001 High Risk Areas Data Quantity Data Movement To/From Country 5 MB Yes View
2000002 High Risk Organizations Data Quantity Data Movement To/From Organization 1 MB Yes View
2000003 Yousendit Data Quantity Data Movement To/From Organization 1 MB Yes View
2000004 Dropbox Data Quantity Data Movement To/From Organization 1 MB Yes View
2000005 Facebook Data Upload Data Quantity Data Movement To/From Organization 2 MB Yes View
2000006 High Risk Connections Connection Count Data Movement To/From Country 50 CON Yes View
2000007 Server Data Loss Data Quantity Data Movement To/From IP Subnet 5 MB Yes View
2000008 High Risk Transfer Data Quantity Data Movement To/From IP Subnet 2 MB Yes View
2000009 Server Data Loss Data Quantity Data Movement To/From Country 10 MB Yes View
2000010 Unusual Data Behavior Data Quantity Abnormal Data Behavior 25% DEV No View
2000011 High Risk Transfers Data Quantity Data Movement To/From IP Subnet 5 MB Yes View
© 2013 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 33 – Behavioral DLP

1.4.4.4 Protected Objects

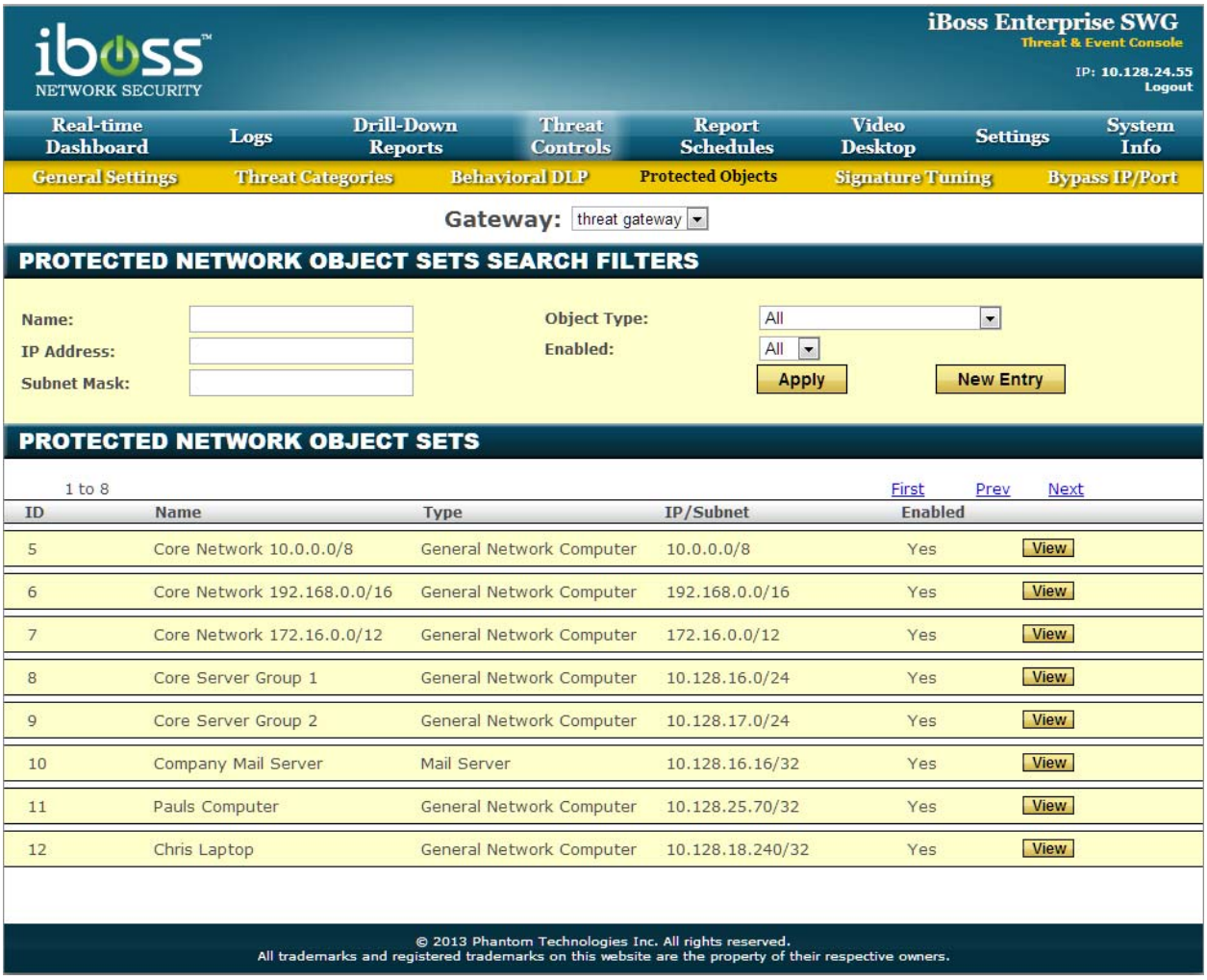

iboss NETWORK SECURITY
iBoss Enterprise SWG
Threat & Event Console
IP: 10.128.24.55
Logout
Real-time Dashboard
Logs
Drill-Down Reports
Threat Controls
Report Schedules
Video Desktop
Settings
System Info
General Settings
Threat Categories
Behavioral DLP
Protected Objects
Signature Tuning
Bypass IP/Port
Gateway: threat gateway
PROTECTED NETWORK OBJECT SETS SEARCH FILTERS
Name:
IP Address:
Subnet Mask:
Object Type: All
Enabled: All
Apply
New Entry
PROTECTED NETWORK OBJECT SETS
1 to 8
First Prev Next
ID Name Type IP/Subnet Enabled
5 Core Network 10.0.0.0/8 General Network Computer 10.0.0.0/8 Yes View
6 Core Network 192.168.0.0/16 General Network Computer 192.168.0.0/16 Yes View
7 Core Network 172.16.0.0/12 General Network Computer 172.16.0.0/12 Yes View
8 Core Server Group 1 General Network Computer 10.128.16.0/24 Yes View
9 Core Server Group 2 General Network Computer 10.128.17.0/24 Yes View
10 Company Mail Server Mail Server 10.128.16.16/32 Yes View
11 Pauls Computer General Network Computer 10.128.25.70/32 Yes View
12 Chris Laptop General Network Computer 10.128.18.240/32 Yes View
© 2013 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 34 – Protected Objects

1.4.4.5 Signature Tuning

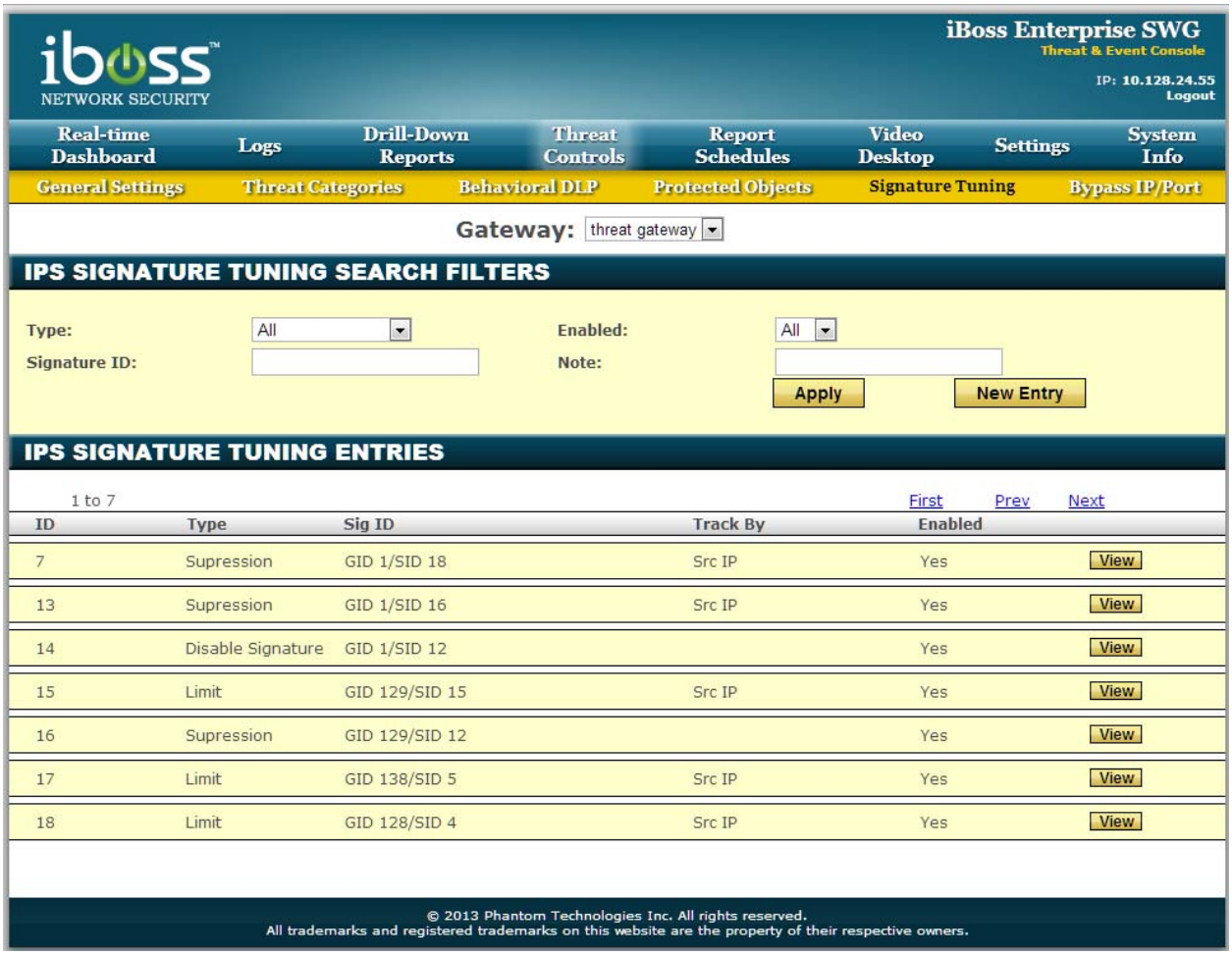


Figure 35 – Signature Tuning

1.4.4.6 Bypass IP/Port

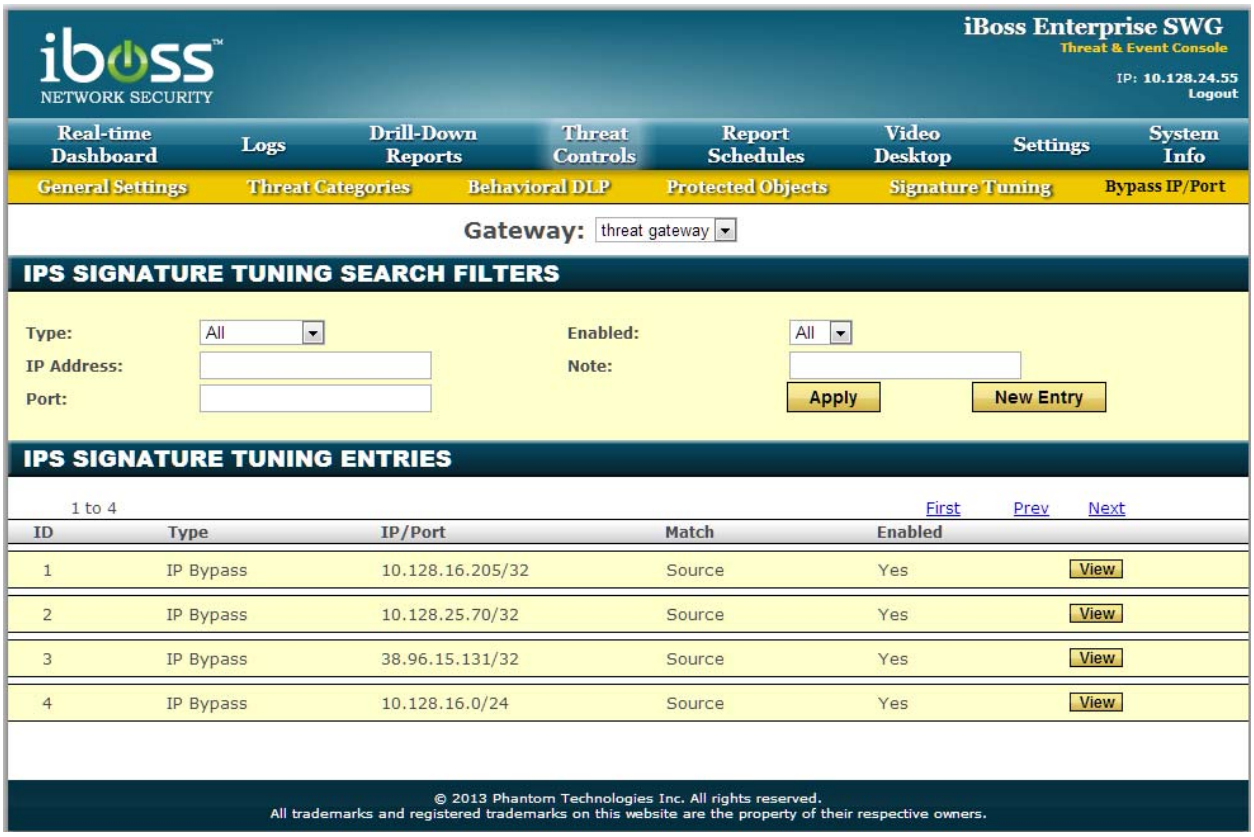


Figure 36 – Bypass IP/Port

1.4.5 Report Schedules

This section allows for the configuration of report generation schedules. Schedules allow you to generate reports for a specified interval of time and have them stored or emailed on a recurring basis. Report schedules also allow for the daily report to be emailed daily to specified recipients.

Figure 37 - Report Schedules

1.4.5.1 Deleting Report Schedules

You can select and delete any report schedule on this page by clicking on the “Remove” button next to the report schedule or selecting the checkboxes of the report schedules you wish to delete and clicking on the “Delete Selected” button. This will terminate the schedule immediately.

1.4.5.2 Editing Report Schedules

To edit a report schedule, click on the edit button next to the report schedule you wish to edit. This will take you to the report schedule editing screen. This screen is similar to adding a report schedule which is detailed in the next sections.

1.4.5.3 Report Schedule Processing

Report schedules are processed when the “Next Processing Time” has been reached which is detailed next to the report schedule. The scheduler will automatically adjust the next processing time automatically. If there are multiple schedules due to be processed at the same time, only one report schedule will be processed at a time. The others will be queued and each processed one at a time until all of the due schedules have been processed.

1.4.5.4 Report Schedule Types

There are two report schedule types, daily report email schedules and custom generated report schedules. Daily report email schedules allow you to email the auto-generated daily reports to specified recipients. It also allows you to enter a customized email message for the email. Custom generated report schedules allow you to create a custom report on a schedule that includes specific statistics, user groups, and more. You can additionally have the custom report emailed whenever a generation occurs.

1.4.5.5 Creating a Report Schedule

To create a report schedule, click on the “Create New Report Schedule” located at the bottom of the report schedule list.

1.4.5.5.1 *General Information*

The general information section allows you enter the following information:

Schedule Name	This is the name you would like to give this schedule. (required)
Description	This allows for a short description of this schedule.
Run Type	The options are Recurring Schedule or Single Run Schedule.
Active	This is the option to turn the schedule active or inactive.
Schedule Type	This indicates the type of report schedule you would like to create. Report schedule types are described above. Daily report schedules allow you to email the auto-generated reports to specified email addresses while custom report schedules allow for the generation of custom reports on a schedule. You may also choose Url List Email Report Schedule.
Format (if Url List Email Report chosen)	This is the format in which the URL list will be emailed. Options are Html and Tab Separated Values TSV.

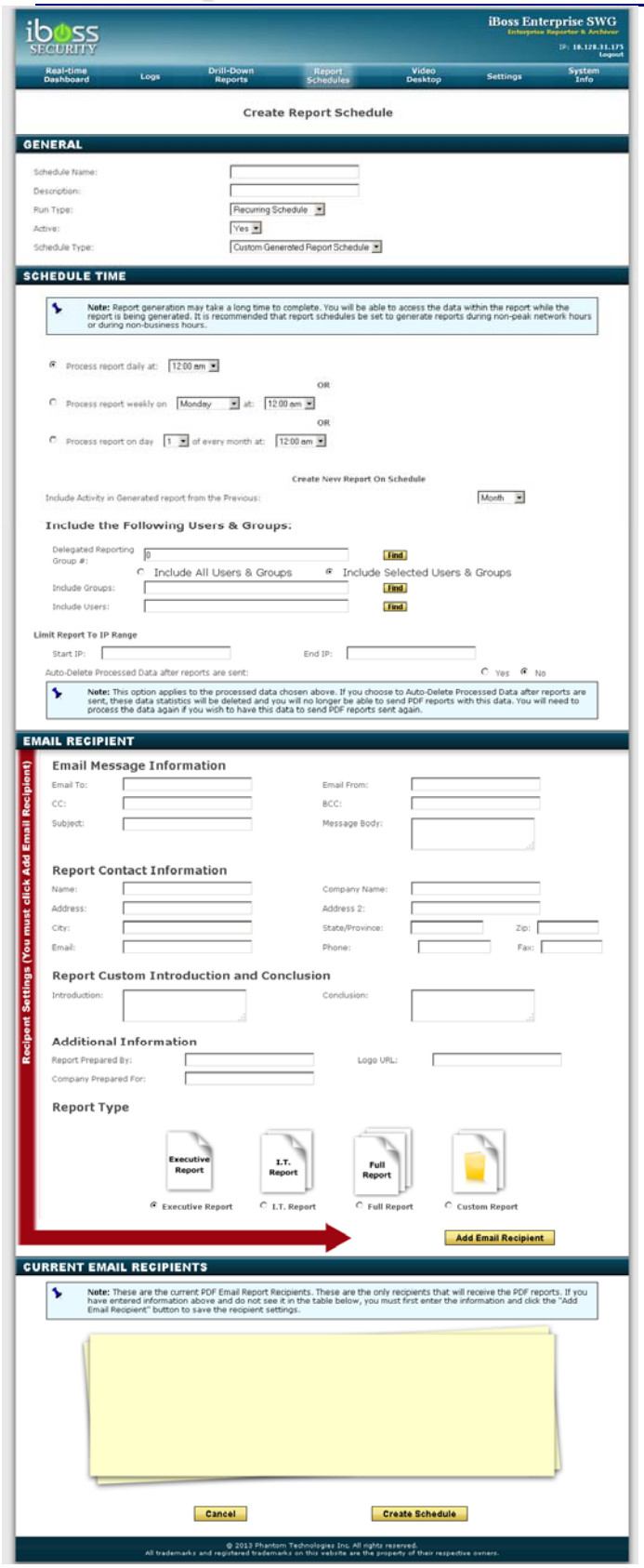

iBoss Enterprise SWG
Real-time Dashboard
Logs
Drill-Down Reports
Report Schedules
Video Desktop
Settings
System Info
Create Report Schedule
GENERAL
Schedule Name:
Description:
Run Type:
Recurring Schedule
Active:
Yes
Schedule Type:
Custom Generated Report Schedule
SCHEDULE TIME
Note: Report generation may take a long time to complete. You will be able to access the data within the report while the report is being generated. It is recommended that report schedules be set to generate reports during non-peak network hours or during non-business hours.
Process report daily at:
12:00 am
OR
Process report weekly on
Monday
at:
Process report on day
of every month at:
Create New Report On Schedule
Include Activity in Generated report from the Previous:
Month
Include the Following Users & Groups:
Delegated Reporting Group #:
Include All Users & Groups
Include Selected Users & Groups
Include Groups:
Include Users:
find
Limit Report To IP Range
Start IP:
End IP:
Auto-Delete Processed Data after reports are sent:
Yes
No
Note: This option applies to the processed data chosen above. If you choose to Auto-Delete Processed Data after reports are sent, these data statistics will be deleted and you will no longer be able to send PDF reports with this data. You will need to process the data again if you wish to have this data to send PDF reports sent again.
EMAIL RECIPIENT
Recipient Settings (You must click Add Email Recipient)
Email Message Information
Email To:
CC:
Subject:
Email From:
BCC:
Message Body:
Report Contact Information
Name:
Address:
City:
Email:
Company Name:
Address 2:
State/Province:
Zip:
Phone:
Fax:
Report Custom Introduction and Conclusion
Introduction:
Conclusion:
Additional Information
Report Prepared By:
Company Prepared For:
Logo URL:
Report Type
Executive Report
I.T. Report
Full Report
Custom Report
Add Email Recipient
CURRENT EMAIL RECIPIENTS
Note: These are the current PDF Email Report Recipients. These are the only recipients that will receive the PDF reports. If you have entered information above and do not see it in the table below, you must first enter the information and click the "Add Email Recipient" button to save the recipient settings.
Cancel
Create Schedule
© 2013 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 38 - Create a Report Schedule

1.4.5.5.2 *Daily Report Email Schedule Settings*

The options available for the daily report email schedule differ from the custom daily report. The daily report email schedule occurs once daily. You must specify email settings and the time you would like to have the daily report schedule processed. Daily report email schedules will contain information for the current day up to the time selected.

1.4.5.5.2.1 Report Schedule Email Settings

This section allows you to enter the details of where you would like to have the email sent to when it is ready. You can include a custom message in the email message body to create specialized reports.

1.4.5.5.2.1.1 Email Message Information

Enter the email information including the recipient, sender, cc, bcc, subject, and message body. This will send the email to another person which looks like it comes from you with a personalized message.

1.4.5.5.2.1.2 Report Contact Information

This information shows up on the cover page of the Emailed PDF Report. Enter the Name, Company Name, Address, City, State, Zip, Email, Phone and Fax.

1.4.5.5.2.1.3 Report Custom Introduction and Conclusion

This information shows up on the second page for the introduction and the last page which is the conclusion. Enter a custom introduction and a custom conclusion.

1.4.5.5.2.1.4 Additional Information

This information shows who the report was prepared by, add a logo, and who it was prepared for. This allows you to customize the report to show that you were the one who prepared it and who it was prepared for. The Logo URL allows you to add a link to an image (.gif or .jpg) to the cover page of the iBoss Report.

1.4.5.5.2.1.5 Report Type

This allows you to choose which type of report to send. There are four options to choose from: Executive, I.T., Full, and Custom. The Executive report has the least information in the report but is used for a quick overview. The I.T. Report show more information such as IP statistics, Port statistics, Application Statistics, and Bandwidth statistics. The Full Report shows all of the contained data. The Custom Report allows you to choose which you may choose which options to include in the report.

1.4.5.5.3 *Custom Generated Report Schedule Settings*

The custom report schedule settings involve configuring extra parameters in addition to those for the daily report schedule settings. The custom report schedule will generate a new report on the schedule (unlike the daily report email schedule).

1.4.5.5.3.1 General Settings

The general information section allows you enter the following information:

Schedule Name	This is the name you would like to give this schedule.
Description	This allows for a short description of this schedule.
Schedule Type	This indicates the type of report schedule you would like to create. Report schedule types are described above. Daily report schedules allow you to email the auto-generated reports to specified email addresses while custom report schedules allow for the generation of custom reports on a schedule.

1.4.5.5.3.2 Statistics

This section allows you to configure which statistics you would like in the custom generated report. The following are statistic options:

Web Stats	Web stats include statistics relating to web browsing activity. This includes top visited domains, top blocked domains, websites visited, and website category statistics.
Port Stats (More Logging)	Port Stats include statistics relating to TCP and UDP port usage on the network. This includes top used ports, top blocked ports, etc.
IP Stats (More Logging)	IP Stats include statistics relating to IP traffic on the network. This includes top accessed IP Addresses, top blocked IP Addresses, etc.
Bandwidth Stats	Bandwidth Stats include statistics relating to general bandwidth usage such as overall, downstream and upstream usage.
Application Stats (More Logging)	Application Stats include statistics specific to applications used on the network.

Note: Selecting More Performance or External Report Manager from within the iBoss Report Settings will only report Web and Bandwidth Statistics.

1.4.5.5.3.3 Email Settings

The email settings allow you to configure options relating to the emailing of the generated report. The following describes the settings in this section.

Email Report To	This is the email address where you would like the report sent to. You can use a semicolon between email addresses to add multiple recipients.
Email CC	This allows for an email carbon copy to be sent to another recipient.
Email BCC	This allows for an email blank carbon copy to be sent to another recipient.
Email Message Body	This allows you to customize the body of the email message.
Auto-delete after report is sent	If this option is enabled, the generated report will automatically be deleted once the report is emailed. This can be used to save disk space and to reduce the number of used generated reports.

1.4.5.5.3.4 Report Schedule Time

This section allows you to configure what time you would like the report schedule to run and the email report sent. There are several options for this section.

You can choose to have the report sent daily at a specified time, weekly at a specified time, or on a specific day of the month at a specified time. Select the appropriate option and configure the time you would like to have this report generated and emailed.

1.4.5.5.3.5 Users

This section allows you to select which user groups will be included in the report. All users inside the selected groups will be included in the generated report. The *Other group contains miscellaneous traffic that might not have been identified on the network.

1.4.5.5.3.6 Create the Report Schedule

When you are done configuring the options for the report, click on the “Create Schedule” button on the bottom of the page. This will return you to the report schedules overview page. This page will show the next processing time for the report schedule.

1.4.6 Automatic Desktop Monitor/Control/Record (DMCR)

This is an add-on feature to the iBoss. This section contains the setup the DMCR feature on the iBoss with the computers on your network. The recording, viewing and controlling of desktops is done by integrating with VNC. VNC (Virtual Network Computing) is a desktop sharing application that allows remote access to another computer. There are many programs that are available that offer VNC and is compatible with Mac, Windows, and Linux. We recommend using UltraVNC (uvnc.com).

1.4.6.1 Installing VNC

Once you have downloaded and installed the VNC program on the computer, you will need to configure it. If you already have it installed and setup, you will need to know the port number and password that are in the settings for the VNC program on the computer. If you are first setting it up, you may start the VNC server program and go to the Admin Properties. This will allow you to configure the port, password, and other settings of the VNC program. Please keep the settings you set for this program handy as you will need it to register the computer to the iBoss DMCR feature. Uncheck the options for removing the wallpaper. For Multi viewer connections, select Keep existing connections and check the Allow Loopback Connections. Here is an example of recommended settings:

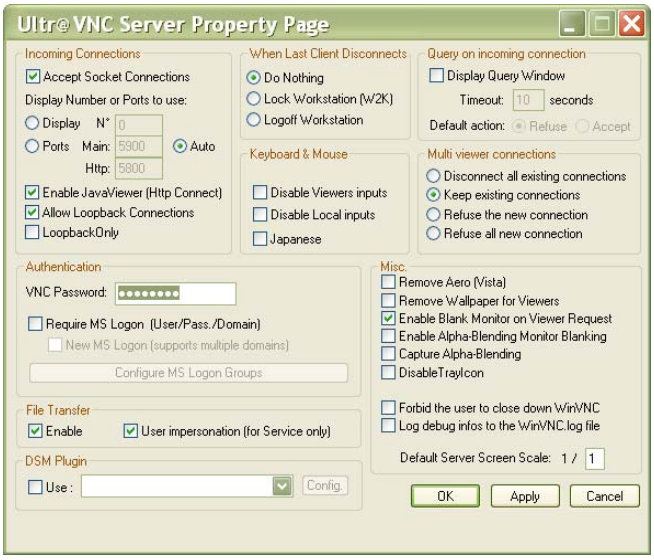


Figure 39 - UVNC Properties

1.4.6.2 Registering a Computer to DMCR

To register a computer to the DMCR feature, you will need to identify the computer through the iBoss. Please refer to the Identifying Computers section for more information. There will be 3 additional settings that are present when identifying computers; Enable/Disable VNC

integration, VNC password, and VNC port. Enter these settings for the computer that you are identifying. Once you have identified this computer and enabled these settings, the computer will show up under the Video Desktop section of the reports.

1.4.6.3 Video Desktop

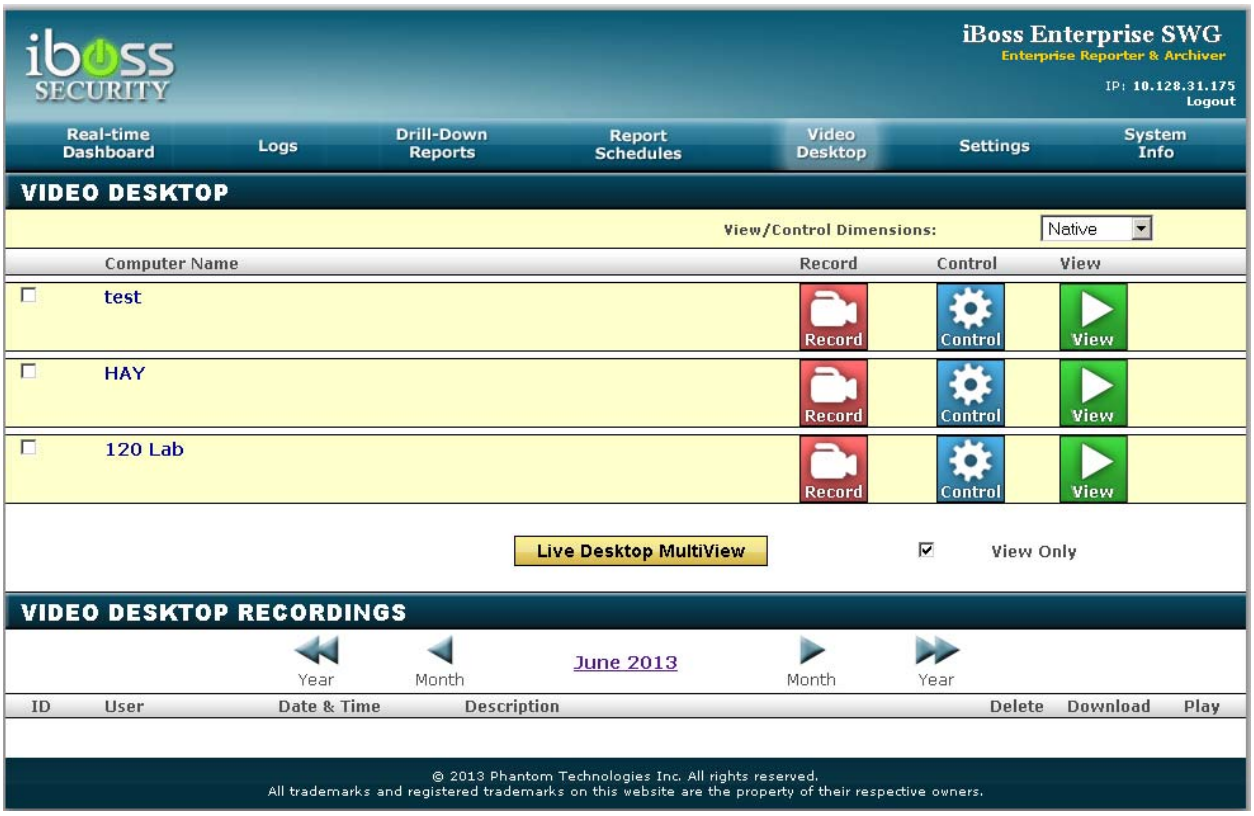


Figure 40 - Video Desktop Monitoring

This section will show you all the computers that are identified with the DMCR feature enabled. You will be able to manually Record, Control and View the desktops straight from this screen.

1.4.6.3.1 *Live Desktop MultiView*

Figure 41 - Live Desktop MultiView

This option allows you to select multiple computers and view up to 10 different screens simultaneously. Select the computers you want to view and click the "Live Desktop MultiView". When viewing the desktops, you may click the Fullscreen button under any of the windows to just view one desktop.

1.4.6.4 Video Desktop Recordings

This section will store all of the desktop recordings. All of the recordings are saved as .swf (Adobe Flash) files. In this section, you may delete, download, or play the recording. Since they are .swf files, you may view them in any standard web browser (with the flash plug-in).

1.4.6.5 Recording Thresholds

Recording thresholds can be set to start recording a user's desktop automatically once a certain violation threshold is reached. For example, if a user goes to an Adult site 5 times within a minute, it will start recording their desktop for 1 minute. These settings can be configured within the iBoss interface, under the Report Settings in Preferences.

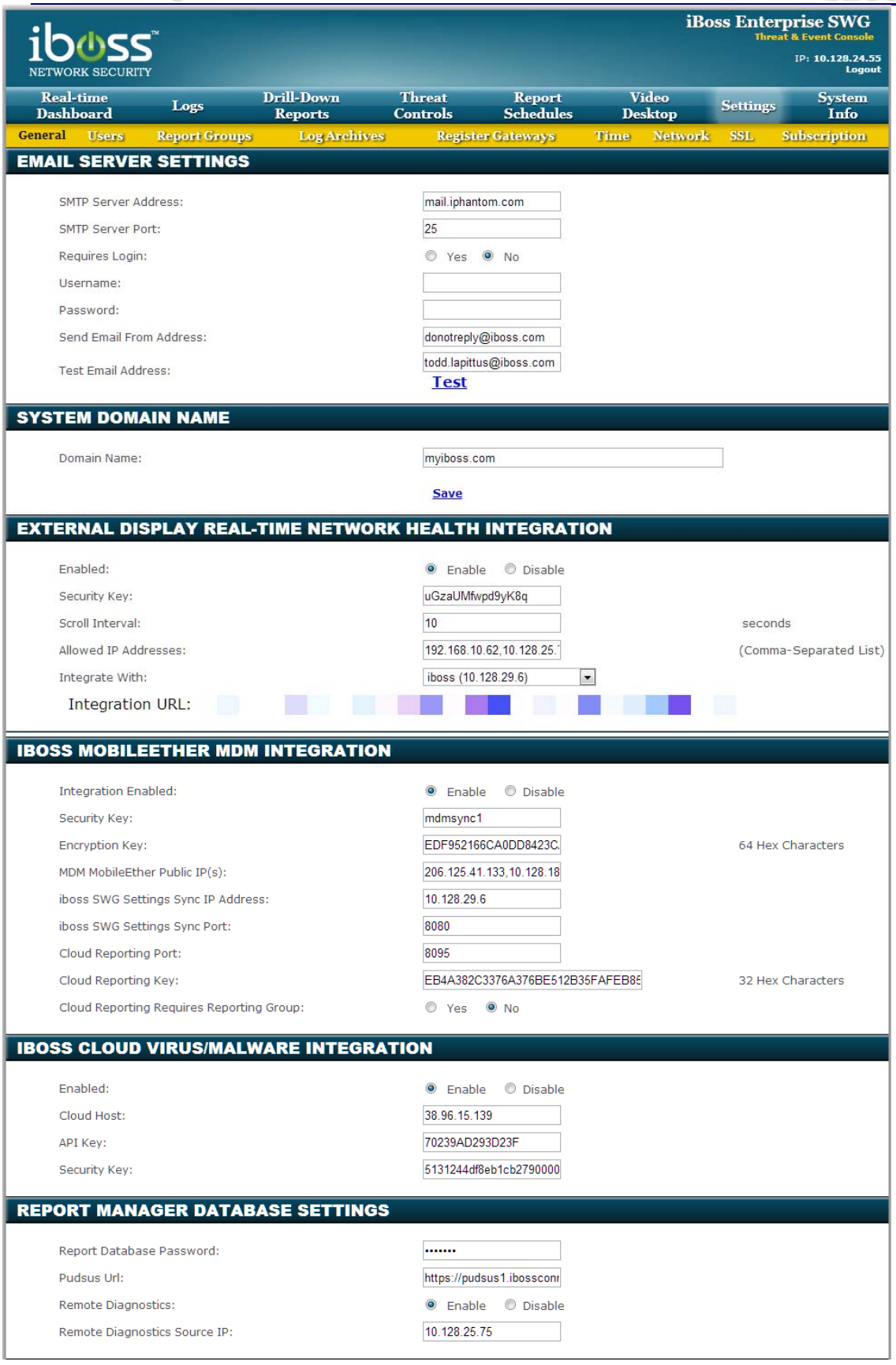
Please refer to the Video Desktop Recording Settings section for more information.

1.4.7 Settings

This section holds several sub-sections for settings.

1.4.7.1 General

This section contains settings used globally for the report manager which include email server settings and other configurable options. Before any email report can be sent via email, the email server settings must be configured.


iboss NETWORK SECURITY
iBoss Enterprise SWG
Threat & Event Console
IP: 10.128.24.55
Logout
Real-time Dashboard
Logs
Drill-Down Reports
Threat Controls
Report Schedules
Video Desktop
Settings
System Info
General
Users
Report Groups
Log Archives
Register Gateways
Time
Network
SSL
Subscription
EMAIL SERVER SETTINGS
SMTP Server Address: mail.iphantom.com
SMTP Server Port: 25
Requires Login: Yes No
Username:
Password:
Send Email From Address: donotreply@iboss.com
Test Email Address: todd.lapittus@iboss.com
Test
SYSTEM DOMAIN NAME
Domain Name: myiboss.com
Save
EXTERNAL DISPLAY REAL-TIME NETWORK HEALTH INTEGRATION
Enabled: Enable Disable
Security Key: uGzaUMfwpd9yK8q
Scroll Interval: 10 seconds
Allowed IP Addresses: 192.168.10.62,10.128.25. (Comma-Separated List)
Integrate With: iboss (10.128.29.6)
Integration URL:
IBOSS MOBILEETHER MDM INTEGRATION
Integration Enabled: Enable Disable
Security Key: mdmsync1
Encryption Key: EDF952166CA0DD8423C 64 Hex Characters
MDM MobileEther Public IP(s): 206.125.41.133,10.128.18
iboss SWG Settings Sync IP Address: 10.128.29.6
iboss SWG Settings Sync Port: 8080
Cloud Reporting Port: 8095
Cloud Reporting Key: EB4A382C3376A376BE512B35FAFEB85 32 Hex Characters
Cloud Reporting Requires Reporting Group: Yes No
IBOSS CLOUD VIRUS/MALWARE INTEGRATION
Enabled: Enable Disable
Cloud Host: 38.96.15.139
API Key: 70239AD293D23F
Security Key: 5131244df8eb1cb2790000
REPORT MANAGER DATABASE SETTINGS
Report Database Password: .....
Pudsus Url: https://pudsus1.ibossconr
Remote Diagnostics: Enable Disable
Remote Diagnostics Source IP: 10.128.25.75

SNMP SETTINGS

SNMP Enabled: (•) Yes ( ) No

SNMP Community: ibossthreatconsole

Allowed Query Subnet: 10.128.0.0/16 (10.20.30.0/24)

Save

REPORT MAINTENANCE SETTINGS

Perform Maintenance At: 2:00 AM Daily

Maximum time to perform maintenance: 2 Hours

Hold Logs Before Deleting: 0 days (0 = delete when needed)

Max URL Log Partition Size: 1250 MB

Max Total URL Log Size: 47500 MB

Max Bandwidth Parition Size: 1000 MB

Max Total Bandwidth Log Size: 3000 MB

Shrink Database By 25 % when full.

Automated Log Rolling Schedule

(•) Disabled

( ) Roll logs daily at: 12:00 am

( ) Roll logs weekly on Sunday at: 12:00 am

( ) Roll logs on day 1 of every month at: 12:00 am

Last Run Time:

Next Run Time: Wed Jan 01 00:00:00 PST 2014

BACKUP TO NETWORK SHARE

Backup Logs To Share When Deleted: No

SMB Folder Name:

SMB User Name:

SMB Password:

SMB User Domain:

Reports Backup Alerts Email:

LDAP SETTINGS

LDAP Enabled: Yes Test

Host/IP: 10.128.30.36

Port: 389

Admin Username: administrator@ibossdoma

Admin Password: ••••••••••

Search Base: dc=ibossdomain2003,dc=

Common Name Key: cn

Match Type: Group Membership And OU

Group Key: memberOf

Group Match Sub Key: CN

Email Key: userPrincipalName

DN Match Sub Key: OU

User Search Filter: (sAMAccountName=%s)

Use SSL: No

Allow Self-Signed Certs: Yes

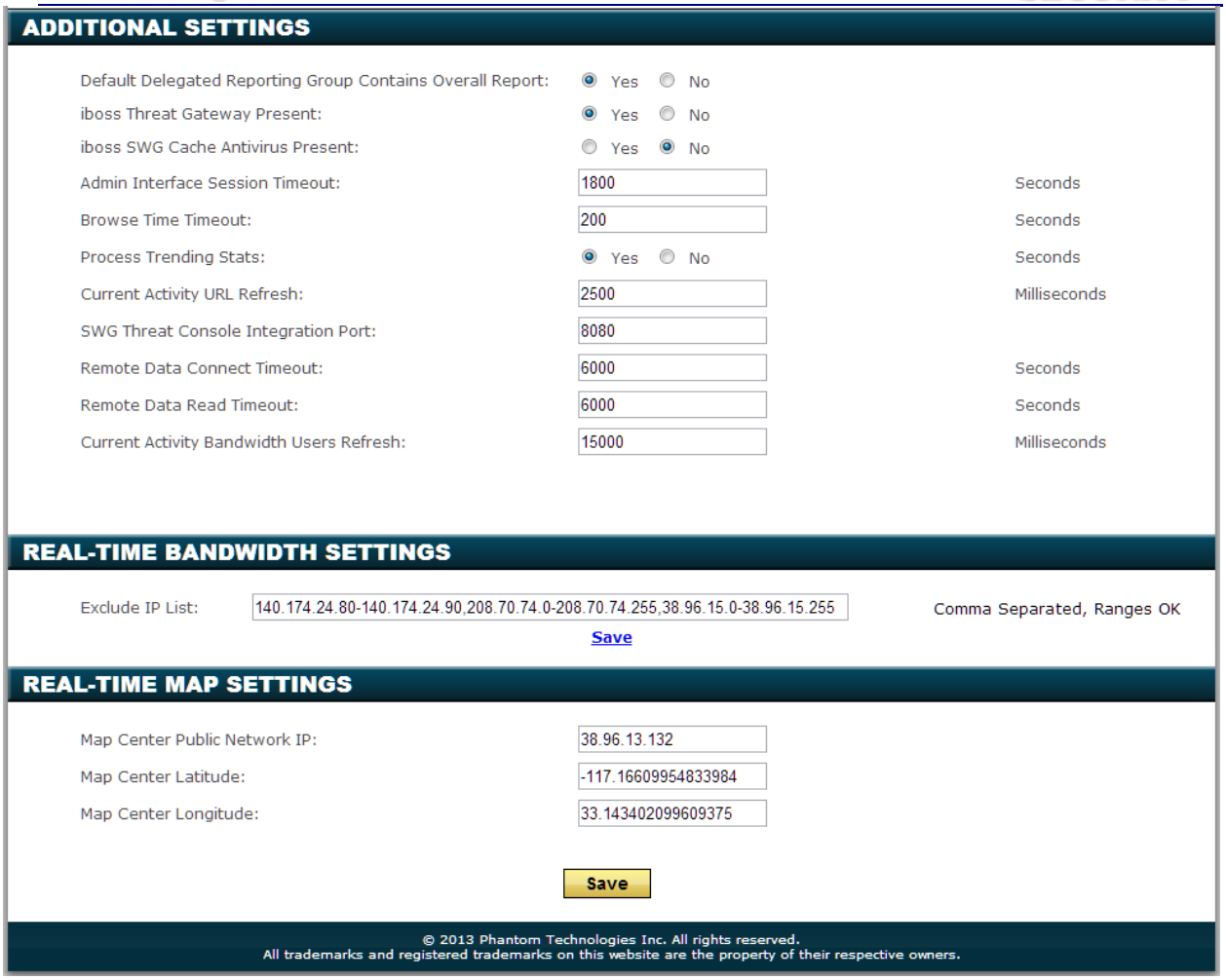

ADDITIONAL SETTINGS
Default Delegated Reporting Group Contains Overall Report: Yes No
iboss Threat Gateway Present: Yes No
iboss SWG Cache Antivirus Present: Yes No
Admin Interface Session Timeout: 1800 Seconds
Browse Time Timeout: 200 Seconds
Process Trending Stats: Yes No Seconds
Current Activity URL Refresh: 2500 Milliseconds
SWG Threat Console Integration Port: 8080
Remote Data Connect Timeout: 6000 Seconds
Remote Data Read Timeout: 6000 Seconds
Current Activity Bandwidth Users Refresh: 15000 Milliseconds
REAL-TIME BANDWIDTH SETTINGS
Exclude IP List: 140.174.24.80-140.174.24.90,208.70.74.0-208.70.74.255,38.96.15.0-38.96.15.255 Comma Separated, Ranges OK
Save
REAL-TIME MAP SETTINGS
Map Center Public Network IP: 38.96.13.132
Map Center Latitude: -117.16609954833984
Map Center Longitude: 33.143402099609375
Save
© 2013 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 42 - Report Manager Settings

1.4.7.1.1 *Email Server Settings*

This section allows you to configure the SMTP server you would like the iBoss to use in order to send email reports.

SMTP Server Address	This is the domain or IP Address of the SMTP mail server you would like to use.
SMTP Server Port	This is the port used to send outgoing mail from your SMTP server.
Requires Login	If your server requires a username and password, set this option to Yes.
Username	This is the username for servers that require login. If the “Requires Login” option is set to false, you can leave this option blank.
Password	This is the password of the user for servers that require login.
Test Email Address	This allows you to test the email settings. Enter a valid email address and click test.

	This will send a test email to the address provided.

1.4.7.1.2 *System Domain Name*

This area allows you to set the domain name of the reporter.

1.4.7.1.3 *External Display Real-Time Network Health Integration*

These settings allow you to configure the Real-Time Network health Display. This display shows the locations and bandwidth for a filter without having to log in to the reporter.

Enabled	Enables the feature
Security Key	This is the security key that is shared with the filter.
Scroll Interval	Controls how often the display scrolls
Allowed IP Addresses	These IP addresses are the only ones allowed to use this service.
Integrate With	This drop down displays all of the filters attached to the reporter. Only one can be selected at a time.

1.4.7.1.4 *IBoss MobileEther MDM Integration*

This section controls the link between the reporter and the MobileEther MDM system. This section controls, not only data reporting for the MDM system, but also integration with directory services and synchronization of filter settings. Please refer to the iBoss MobilEther MDM guide for more details.

Integration Enabled	Enables the feature.
Security Key	This security key is shared with the MDM unit.
Encryption Key	This key is also shared with the MDM unit. 64 Hex characters
MDM MobileEther Public IP(s)	IP addresses of the MDM systems integrated with this reporter.
iBoss SWG Settings Sync IP Addresses	Filters that are associated with this reporter and MDM for filter settings sync.
iBoss SWG Settings Sync Port	Port used for sync. 8080 by default.
Cloud Reporting Port	Port used to integrate with MDM. 8095 by default.
Cloud Reporting Key	Key associated with MDM.

1.4.7.1.5 *IBoss Cloud Virus/Malware Integration*

This section details the settings for integration with Cloud Antivirus/malware protection. Please refer to the iBoss Cloud Antivirus/Malware manual for more information.

Enabled	Enables the feature
Cloud Host	IP address of the Cloud hosting the anti-virus service.
API Key	Key to link to the local program.
Security Key	Key Linking the reporter and cloud.

1.4.7.1.6 *Report Manager Database Settings*

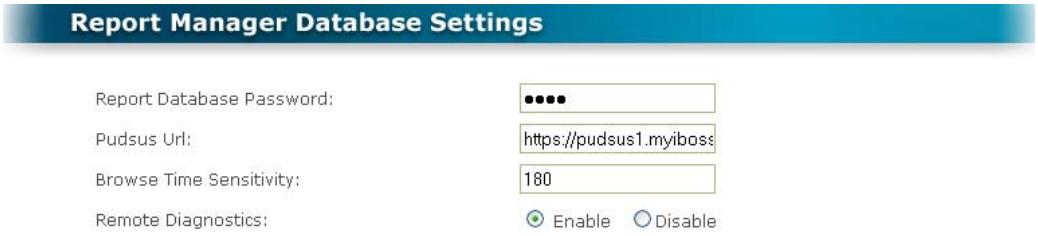


Figure 43 - Report Manager Database Settings

This section allows you to configure the Enterprise Reporter Database Settings for the iBoss to report to.

Report Database Password - The default Password is **ibossdb.** This can be left by default as the Enterprise Reporter will only allow connections from registered iBoss units however, it is recommended to change this password. Keep this password handy as you will need it to register iBoss units to it.

Pudsus Url – This is the URL where the iBoss Enterprise Reporter gets its updates from. Do not change this URL unless told to do so by a Phantom Technologies Technician. This may cause the Enterprise Reporter to function improperly if changed.

Browse Time Sensitivity – This option is for the time usage statistics of how long a URL is counted as being viewed after first accessed. This is only if there is no more traffic after hitting a website as it limits to this amount in seconds.

Remote Diagnostics – This option allows you to enable Remote Diagnostics for a Phantom Technologies technician to assist you remotely.

1.4.7.1.7 *SNMP Settings*

This area configures the SNMP settings. Enabling, the Community and the Allowed Query Subnet are included.

1.4.7.1.8 *Report Maintenance Settings*

These settings allow you to configure the maintenance options for the report manager. Maintenance occurs once per day.

Perform Maintenance At	This is the time you would like maintenance to occur. Configure this option for a time when the network has the lightest load.
Maximum time to perform maintenance	This option allows you to limit the maximum maintenance time. Although maintenance may not take too long to complete, if the report manager is shrinking the database or performing other intensive routines, maintenance may take a long time to complete. It is important that the iBoss is given enough time to complete all of its tasks. The Unlimited option is recommended.
Hold Logs Before Deleting	When it becomes time to delete data, the reporter can hold-off from deleting the URL logs for the specified number of days. The logs will be marked for deletion. 0 deletes the table immediately as needed.
Max URL Log Partition Size	This option is the maximum size of the URL Log size before rolling into another table. Smaller values will increase performance and will generate more tables.
Max Total URL Log Size	This option is the maximum size of all URL logs combined can occupy in the database. Smaller values will increase the amount of time the daily reports will be stored in the database, as more space will be available for reports vs. URL logs.
Max Bandwidth Partition Size	This option is the maximum size of the Bandwidth Log the bandwidth partition tables before rolling into a new table.
Max Total Bandwidth Log Size	This option is the maximum size of all bandwidth logs combined can occupy in the database. Smaller values will increase the amount of time the daily reports will be stored in the database, as more space will be available for reports vs. URL logs.
Shrink Database By % when full	The percentage of the database size that will decrease when full.
Automated Log Rolling Schedule	This option allows you to set a schedule for the Logs to be rolled into a different log. This will make archives in different sections to be able to backup later. You can set it to disabled, daily, weekly or monthly.

1.4.7.1.9 *Backup To Network Share*

These settings allow you to configure the maintenance options for the report manager. Maintenance occurs once per day.

Backup Logs To Share When Deleted	This option allows you to enable the URL log archives to be backed up to a shared folder before it is deleted.

SMB Folder Name	This option allows you to the full path of the backup share folder. You may need to include the IP address in the address.
SMB User Name	This option is for the username used for the backup share folder to be able to connect to it.
SMB Password	This option is for the password for the username used for the backup shared folder.
SMB User Domain	By default may be blank but you may set this to your servers NetBIOS name.
Reports Backup Alerts Emails	This option allows you to send email alerts when backups are made.

1.4.7.1.10 *LDAP Settings*

This section enables integration with directory services for the purposes of both user login and integration with MDM.

LDAP Enabled	Enables the service
Host / IP	This is the domain or IP address of the LDAP server. Example: iphantom.com or 10.0.0.1
Port	This allows you to change the port number that is used to communicate to your LDAP server. Port 389 is most common and is recommended.
Admin Username	This is the Username of an administrative or root user which has administrative rights to your LDAP server. The user must be able to perform searches on your LDAP server. This user is used to look up user logins. Example: administrator@iphantom.com.
Admin Password	This is the password to your LDAP administrator user above. Some special characters are not accepted.
Search Base	This is the base by which searches for users will be made. If you have a large directory you may choose a base other than the top as long as all users that need to be authenticated are under this base. It is recommended that you set this to the top of your LDAP directory. Example: If your LDAP domain is iphantom.com, you would use the following settings: dc=iphantom,dc=com
Common Name Key	'cn' by default.
Match Type	LDAP can match by group name or OU or both.
Group Key	Within LDAP, this string is used for group matching. In AD it is 'memberOf'.
Group Match Sub Key	In AD this is 'CN'.
Email Key	Key for using an e-mail address with LDAP.

	In AD this is 'userPrincipalName'.
DN Match Sub Key	If 'User DN' is included within the 'Match Group Source' option then this key is used to parse the User DN. Active Directory Example: OU
User Search Filter	This is the filter that is used to search for a username in the LDAP server. This filter must result in a single user record. The filter must also contain %s which will be replaced by the username. There must not be any other percent signs in the search filter. Active Directory Example: (sAMAccountName=%s)

Once you have finished entering information, click the Test button. This saves the information as well as tests the information against the LDAP server.

1.4.7.1.11 *Additional Settings*

This setting allows you to configure the email address used for sending Email Alerts to.

Default Delegated Reporting Group Contains Overall Report	This is the option which allows you to include all reporting groups for statistics on the current activity page.
iBoss SWG Intrusion/Malware Present	Activates Sync with iBoss IPS
iBoss SWG Cache Antivirus Present	Activates Sync with Cache Antivirus
Admin Interface Session Timeout	Determines how long the Reporter interface remains logged in with no activity.
Browse Time Timeout	
Process Trending Stats	Turns on and off the process that displays Trending statistics
Current Activity URL Refresh	Determines how often the URL Activity on the Real Time Dashboard updates.
Remote Data API Port	Port for the Remote Data Service
Remote Data Connect Timeout	Connect Timeout setting for the Remote Data Service
Remote Data Read Timeout	Read Timeout setting for the Remote Data Service
Current Activity Bandwidth Users Refresh	How often the badwidth users refresh on the Real Time Dashboard

1.4.7.1.12 *Real-Time Bandwidth Settings*

This area allows you to exclude IPs from the Real Time Bandwidth display, by single IP or range.

1.4.7.1.13 *Real Time Map Settings*

Map Center Public Network IP	External IP of the Reporter
Map Center Latitude	Latitude of the server location
Map Center Longitude	Longitude of the server location

1.4.7.2 Users

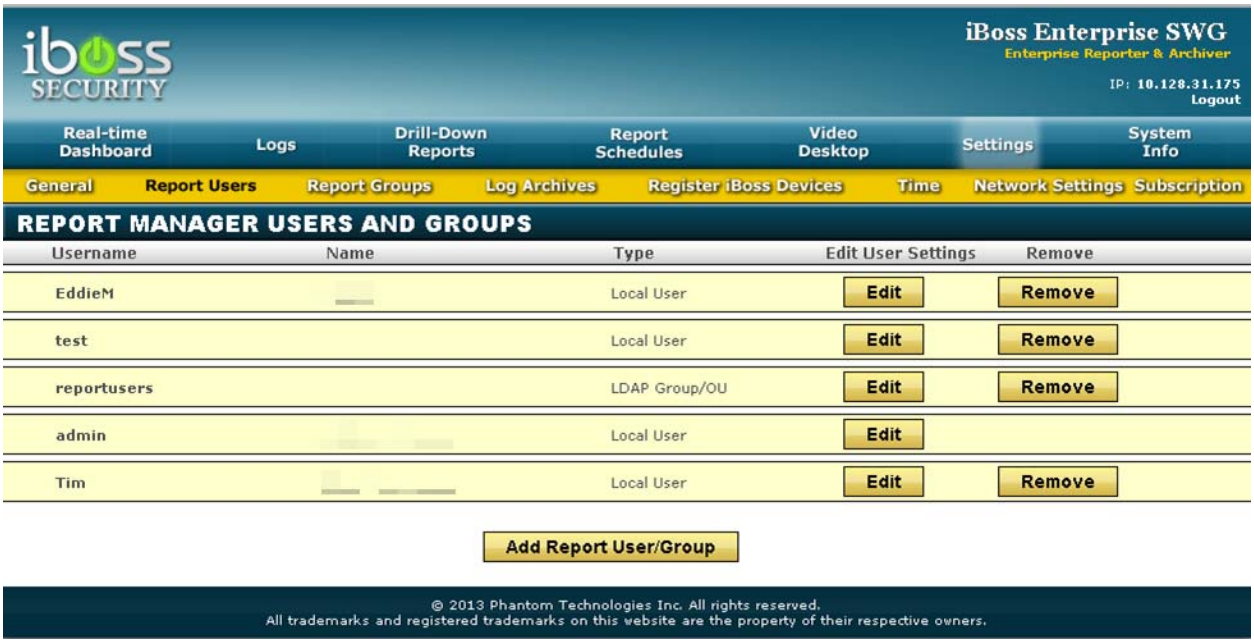


Figure 44 - Report Users

This section allows you to add/edit users that can log into the Enterprise Reporter. The default user is "**admin**" which has no password by default. It is recommended to click "Edit" and set a password for the Administrator.

To add a user, click Add Report User

1.4.7.2.1 *Add Report User*

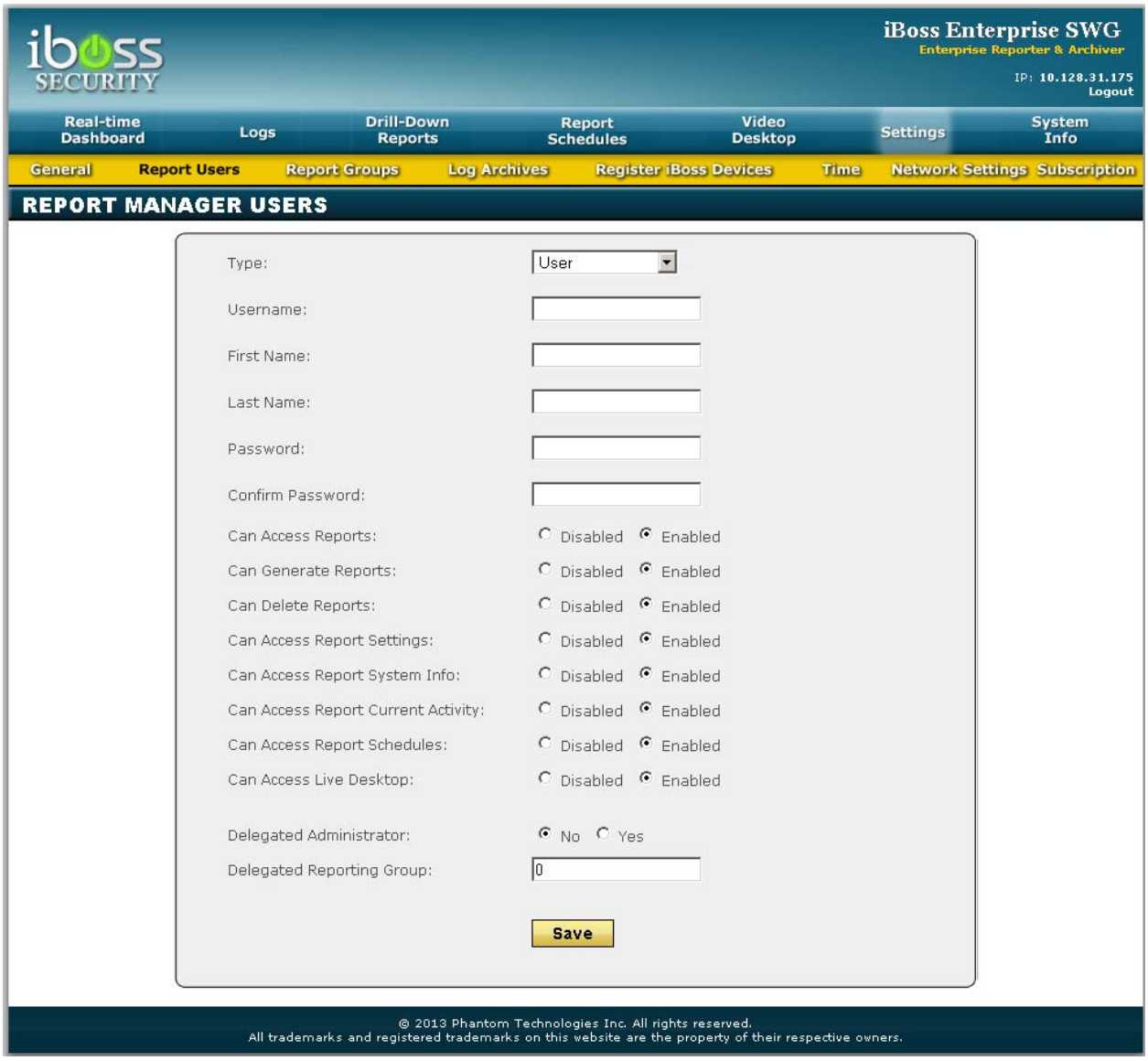


Figure 45 - Add Report Manager User

To add a user, enter the Username, First Name, Last Name, and Password. Then select which sections of the report the user can access. The options to choose from are Can Generate Reports, Can Delete Reports, Can Access Report Settings, Can Access Report System Info, Can Access Report Current Activity, Can Access Report Schedules, and Can Access Live Desktop.

After you are done settings all of the settings, click Save.

To add an LDAP Group, first configure the LDAP settings on the General page, then select LDAP Group in the dropdown.

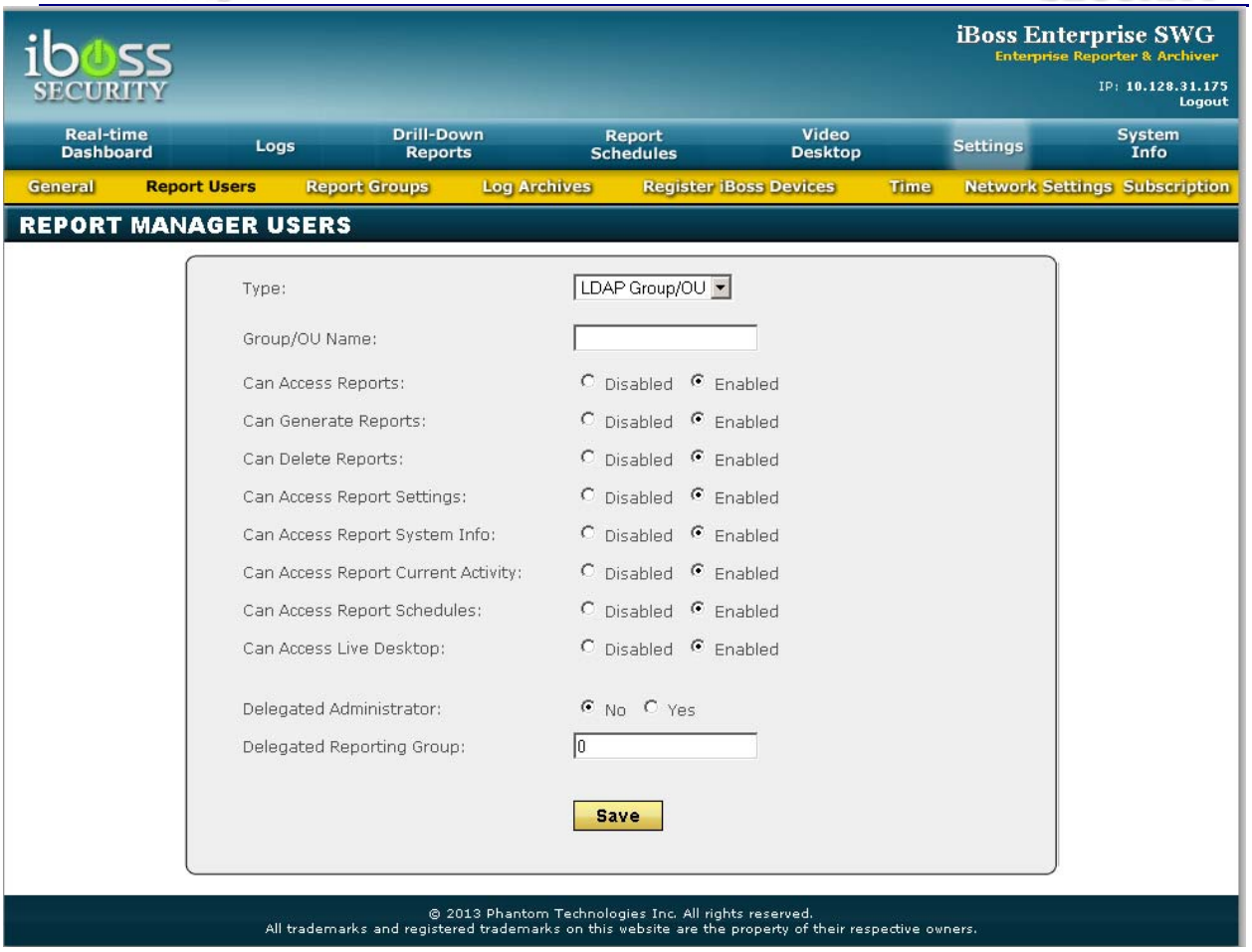


Figure 46 – LDAP User config

All other options remain the same except for the name of the group or OU you want to give report access to.

1.4.7.3 Report Groups

Figure 47 - Report Groups

This section allows you to add/edit Reporting Groups that can log users into separate groups. The Report Users can then be assigned to see just these reporting groups. These delegated admins of the reports will only see the reporting groups assigned to them. The default group is "**Default Group**" and is group # 0. When making a user part of a different reporting group, the user would then be taken out of Default Group # 0 and put into the new reporting group.

To add a reporting group, click Add Reporting Group

1.4.7.3.1 *Add Reporting Group*

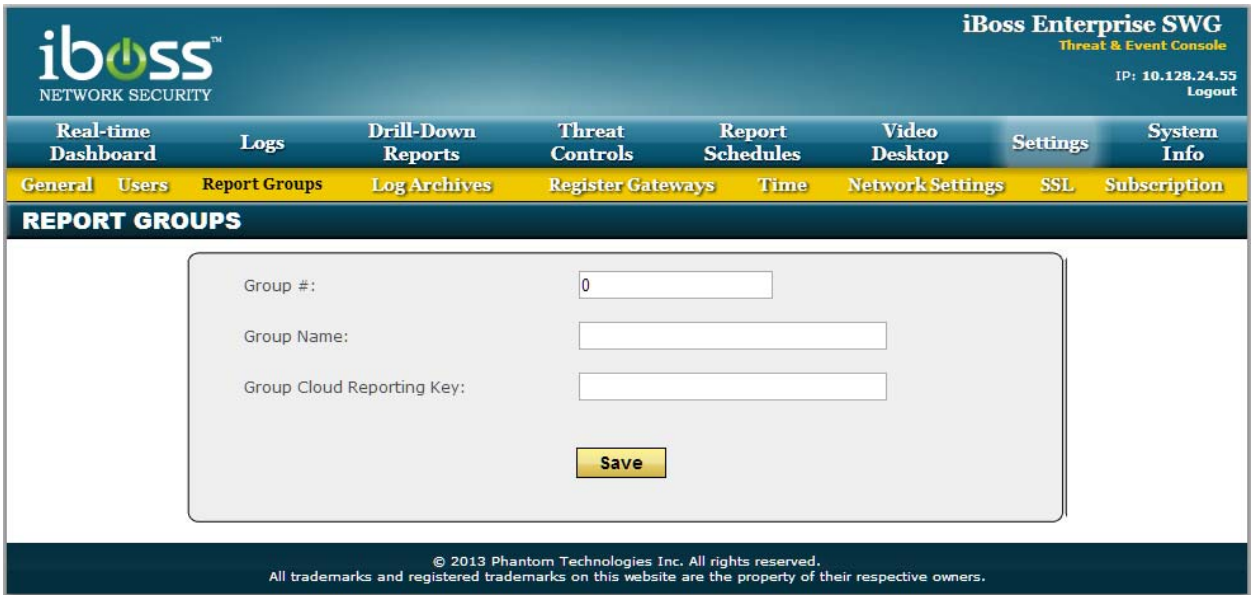


Figure 48 - Add Reporting Group

To add a reporting group, put the group number and group name. If it is a cloud filter, include the Group Cloud Reporting Key.

After you are done settings all of the settings, click Save.

1.4.7.4 Log Archives

This section holds the logs for URLs, Bandwidth and IPS.

1.4.7.4.1 *URL Log Archives*

Figure 49 - Manage URL Log Archives

This section allows you manage the URL logs. You may Roll URL logs into archives. This allows you to bunch URLs and then back them up or delete them.

You may also setup a Backup Share under the General Settings to have the URL Log archives backed up to.

With Backup Share folder setup on the General Settings, the list of backed up URL Log archives will be displayed. If the Backup Share has not yet connected, it may take a couple minutes for this page to load as it is establishing a connection to the backup share.

1.4.7.4.2 *Bandwidth Log Archives*

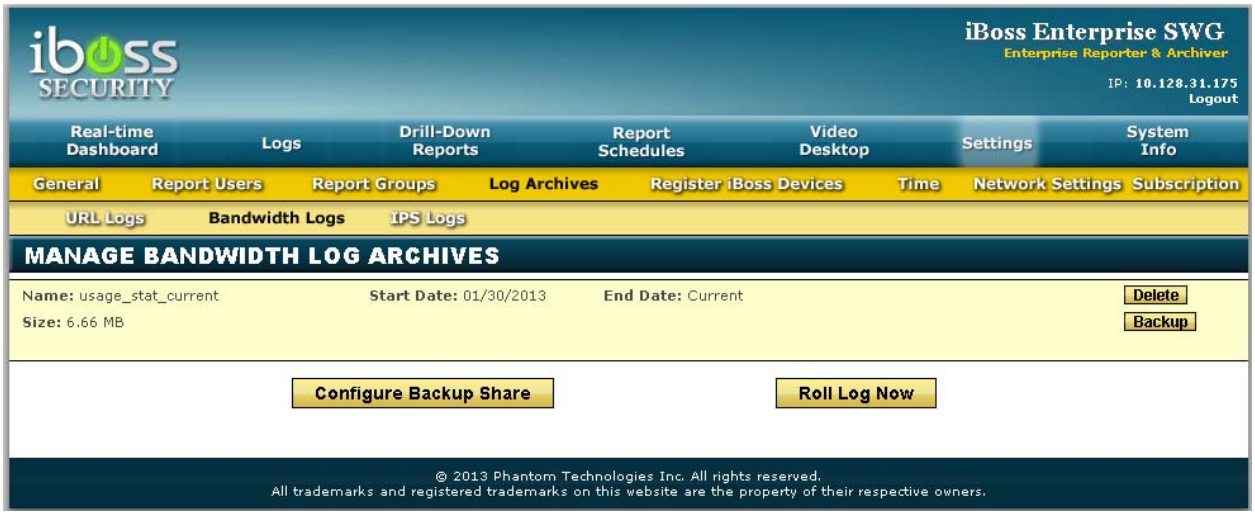


Figure 50 - Manage Bandwidth Log Archives

This section allows you manage the Bandwidth logs. You may Roll Bandwidth logs into archives. This allows you to bunch bandwidth statistics and then back them up or delete them.

You may also setup a Backup Share under the General Settings to have the Log archives backed up to.

With Backup Share folder setup on the General Settings, the list of backed up Bandwidth Log archives will be displayed. If the Backup Share has not yet connected, it may take a couple minutes for this page to load as it is establishing a connection to the backup share.

1.4.7.4.3 *IPS Logs*

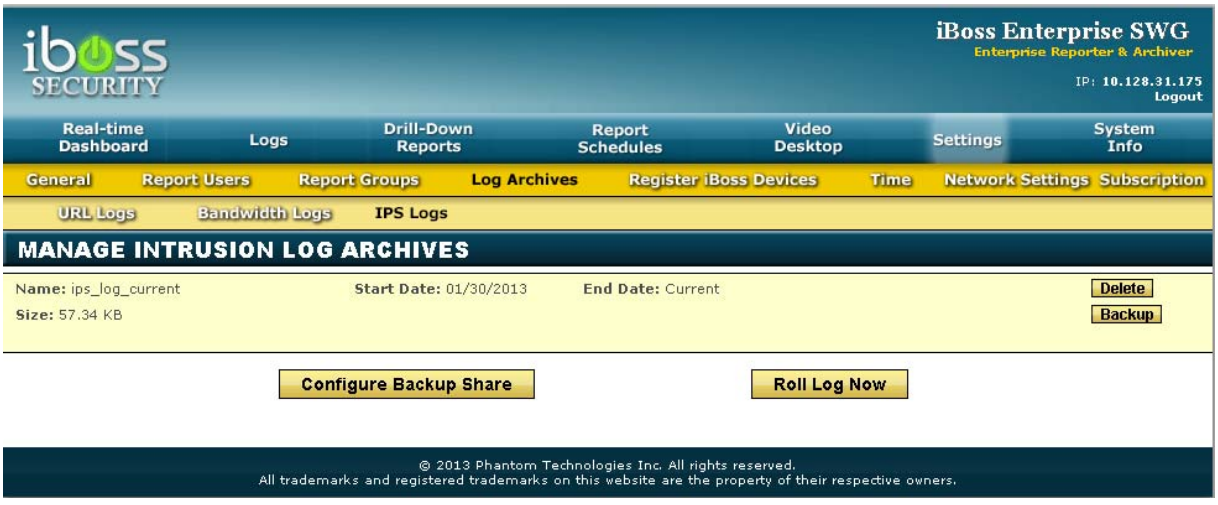


Figure 51 – IPS Logs

This section allows you manage the IPS logs. You may Roll IPS logs into archives. This allows you to bunch bandwidth statistics and then back them up or delete them.

You may also setup a Backup Share under the General Settings to have the Log archives backed up to.

With Backup Share folder setup on the General Settings, the list of backed up Bandwidth Log archives will be displayed. If the Backup Share has not yet connected, it may take a couple minutes for this page to load as it is establishing a connection to the backup share.

1.4.7.5 Register Gateways

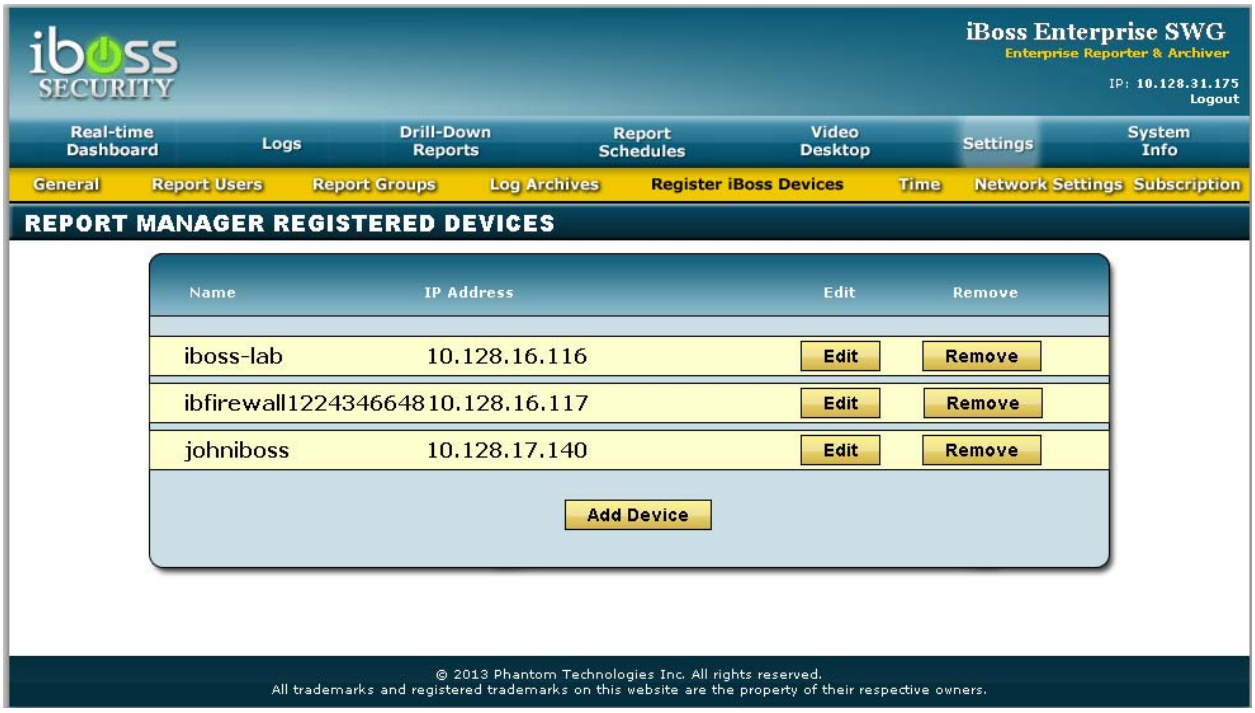


Figure 52 - Register iBoss Devices

This section allows you to add/edit/remove iBoss Devices to log to the external Report Manager. You will need to register any iBoss devices that you wish to have reporting to the external report manager.

To add an iBoss Device, click Add Device.

1.4.7.5.1 *Register Gateway*

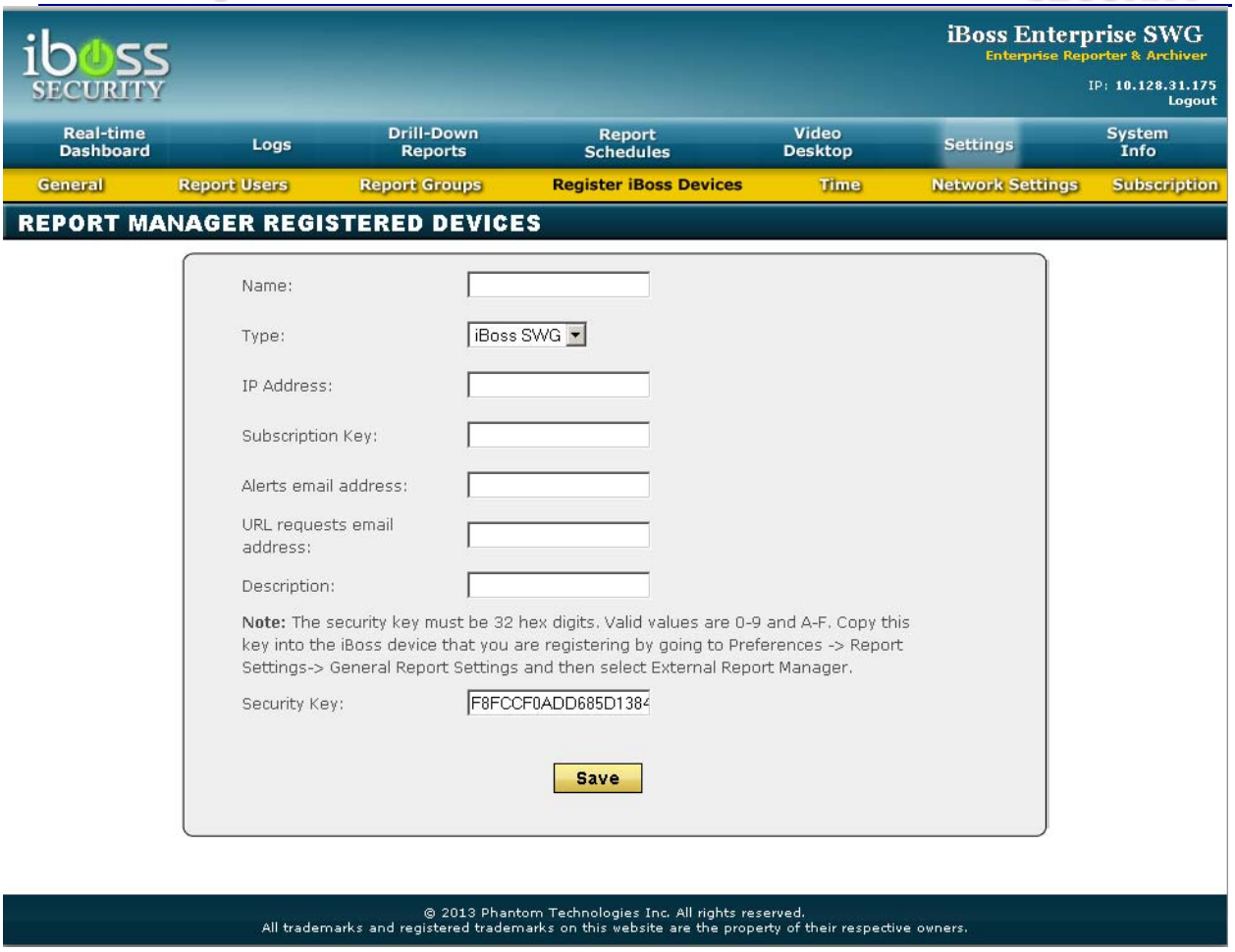


Figure 53 - Register Gateway

To add an iBoss Device, enter the iBoss Device Name, Device IP Address, Description, and Security key. You may change the security key to a 32 hex digit key. **Please keep this key handy as you will need it when registering the iBoss settings to point to the external report manager.**

Please refer to the Report Settings of the iBoss Interface for instructions on how to configure the External Report Manager Settings.

1.4.7.6 Time

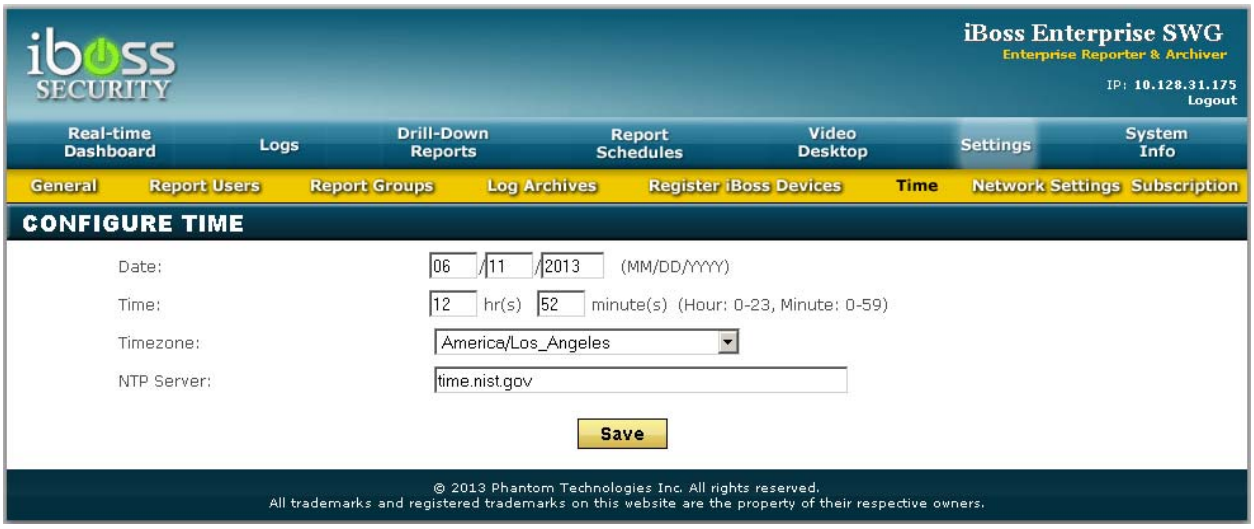


Figure 54 - Configure Time

This section allows you to set the time zone and time for the external report manager. After changing the correct time zone, click Save. The iBoss Enterprise Reporter will need to reboot after saving. In addition, if you have a local NTP server, you can use that instead of the national time server.

1.4.7.7 Network Settings

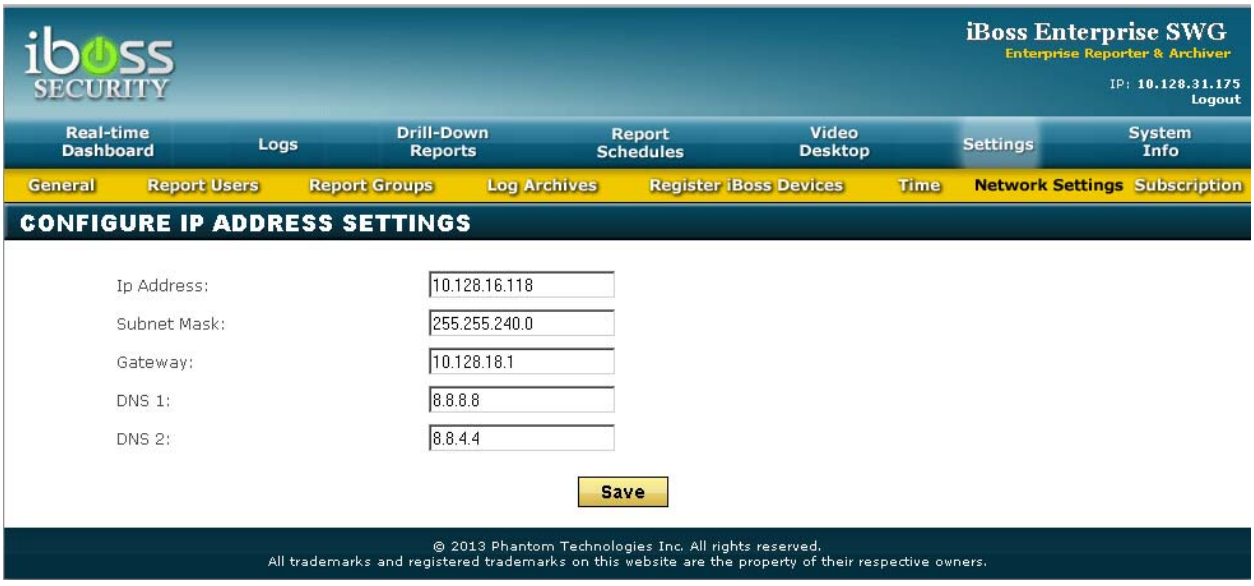


Figure 55 - Configure IP Address Settings

This section allows you to set the network settings for the external report manager. You may set the IP address, Subnet Mask, Gateway, DNS 1, and DNS 2. After entering the settings, click Save. The iBoss Enterprise Reporter will need to reboot after saving.

Default iBoss Enterprise Reporter IP Address Settings

IP Address	192.168.1.20
Subnet Mask	255.255.255.0
Gateway	192.168.1.1
DNS 1	192.168.1.1
DNS 2	0.0.0.0

You may set these settings through the serial console. Please refer to the serial console settings in the iBoss serial console section.

1.4.7.8 SSL

This area allows you to upload certificates for the reporter.

1.4.7.9 Subscription

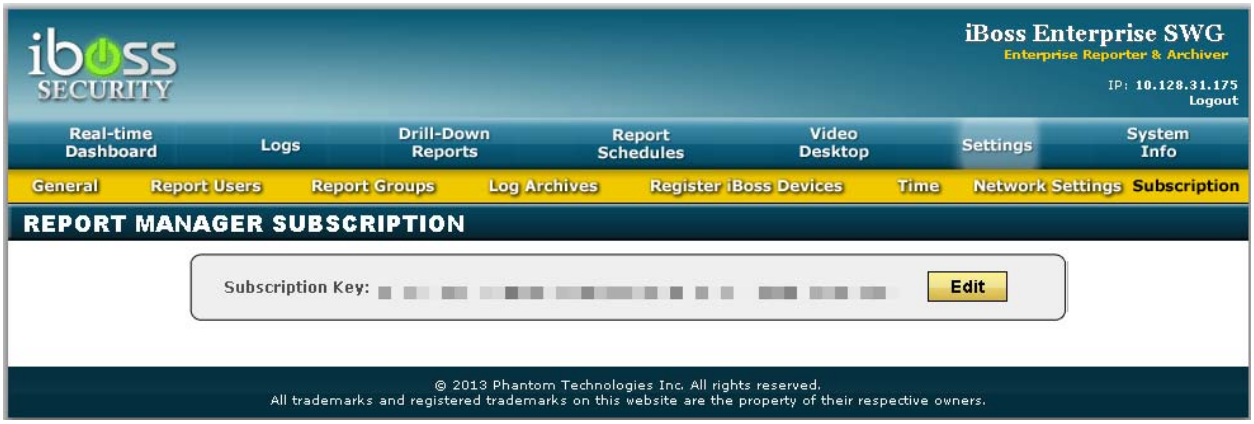


Figure 56 - Subscription

This section allows you to enter the subscription key. You may click Edit to enter the key. Once you enter the key click Edit to save the key and then Confirm. The report manager will need to be connected to the Internet to be able to confirm this key. Please make sure it is plugged into the network to be able to verify the subscription key.

Note: The report manager will not process log data and will not fully function if your subscription is not active.

1.4.8 Report Manager System Information

This section contains system information pertaining to the iBoss. This includes the system log, the system uptime, and the database size. From this page, you can view and clear the system event log. In addition, you can view how much disk space the report manager is consuming and how much disk space is available. When the maximum is reached, the database will automatically shrink on the maintenance interval.

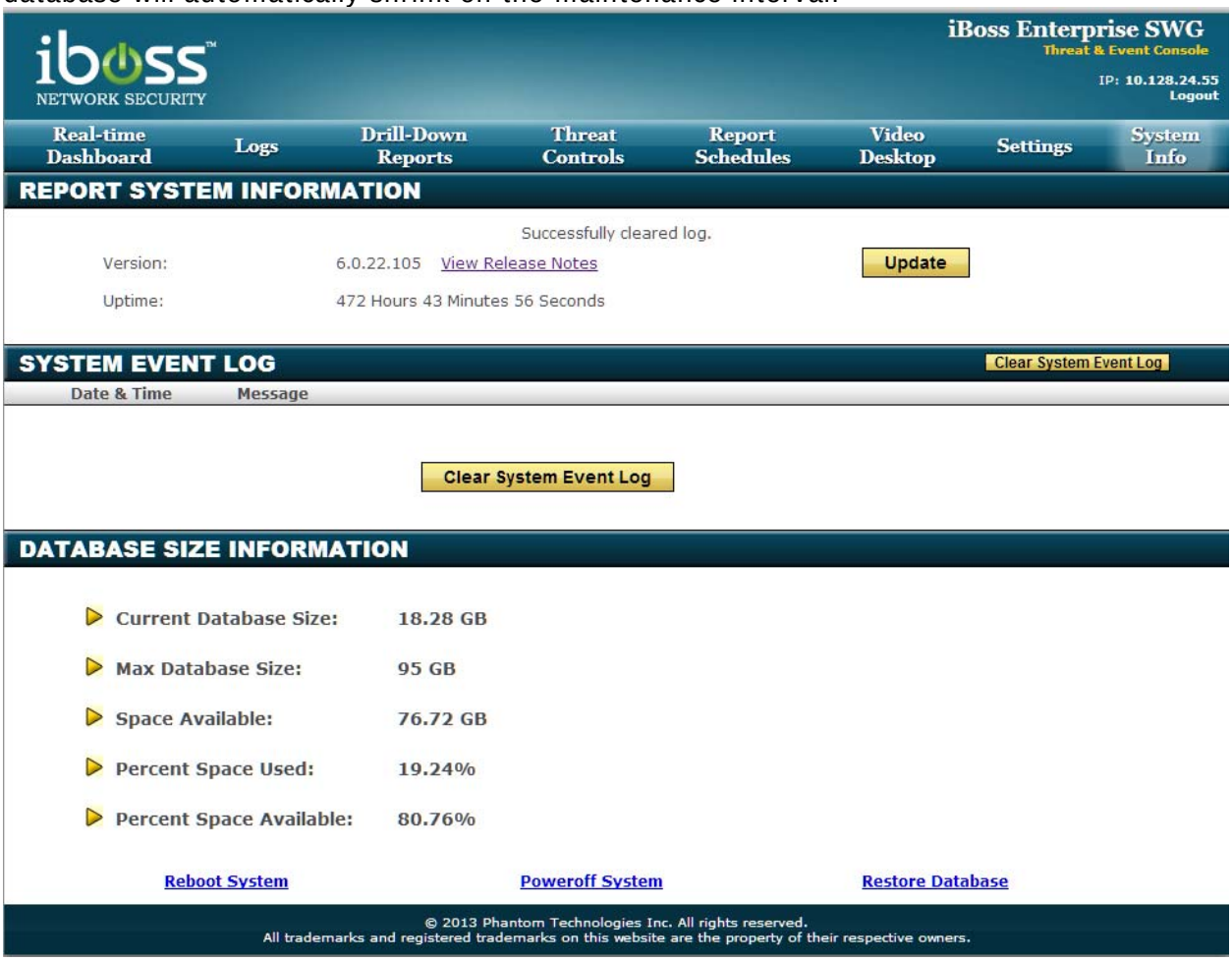


Figure 57 – System Info

1.5 Viewing Reports

You may view reports by clicking on the report you wish to view from the “View Reports” section of the report manager. When you click on the report, you will be taken to the web statistics section of the report.

Most of the items within the report manager are “clickable”. The report manager allows deep drilldown functionality to provide very detailed information very easily.

1.5.1 Report Information Section

When viewing any of the report pages, the report information section will be visible at the top of the page. This section gives you information regarding the current report and allows you to switch between reports easily.

Figure 58 - Report Information Section

The report information bar contains the name of the report, as well as the date range that this report covers.

1.5.1.1 Showing Report Information for Particular Users

Under the option “User”, you have the capability of entering in which users to show the report for. If nothing is typed into the text box, the information in the report pages you are viewing will contain information regarding all users in the report.

If you would like to view information for a particular user in the report, type the username in or click the “Find” button. You can then enter part of the user’s name and click find, this will populate the list of usernames. You can then click select next to the username and then “Done” button once you’re finished. Next, click the “Apply” button to show. Once a user is selected, all statistics on the page pertain to the particular user.

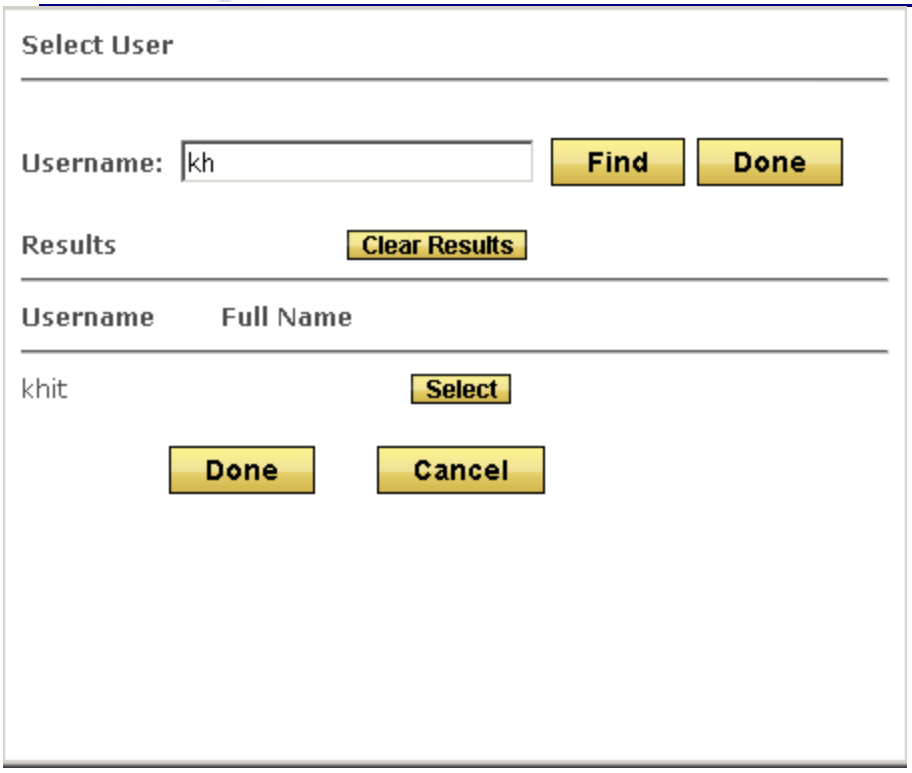


Figure 59 – Find User

Regardless of whether you have all users selected or a particular user, the information presented will look the same and is consistent. The only thing that changes is the information on the page, not the structure.

1.5.1.2 Quickly switching between reports

The top right section of the report information bar has a drop down list which allows you to quickly switch between reports. Simply select a report from the drop down list and the current report page will be updated with the information from the newly selected report. This is useful for comparing information between two or more reports.

1.5.2 Web Usage Statistics

This section contains information related to web browsing. This includes websites visited, top visited domains, top blocked domains, web category usage as well as other statistics. As stated above, most of the items are clickable and can be drilled down for more detail.

Figure 60 - Web Usage Statistics

1.5.2.1 Web Hit Trends

This section shows web hit trends for the current report over time. It displays both Hit Count and Block Count. You can click and drag to zoom into a more specific time.

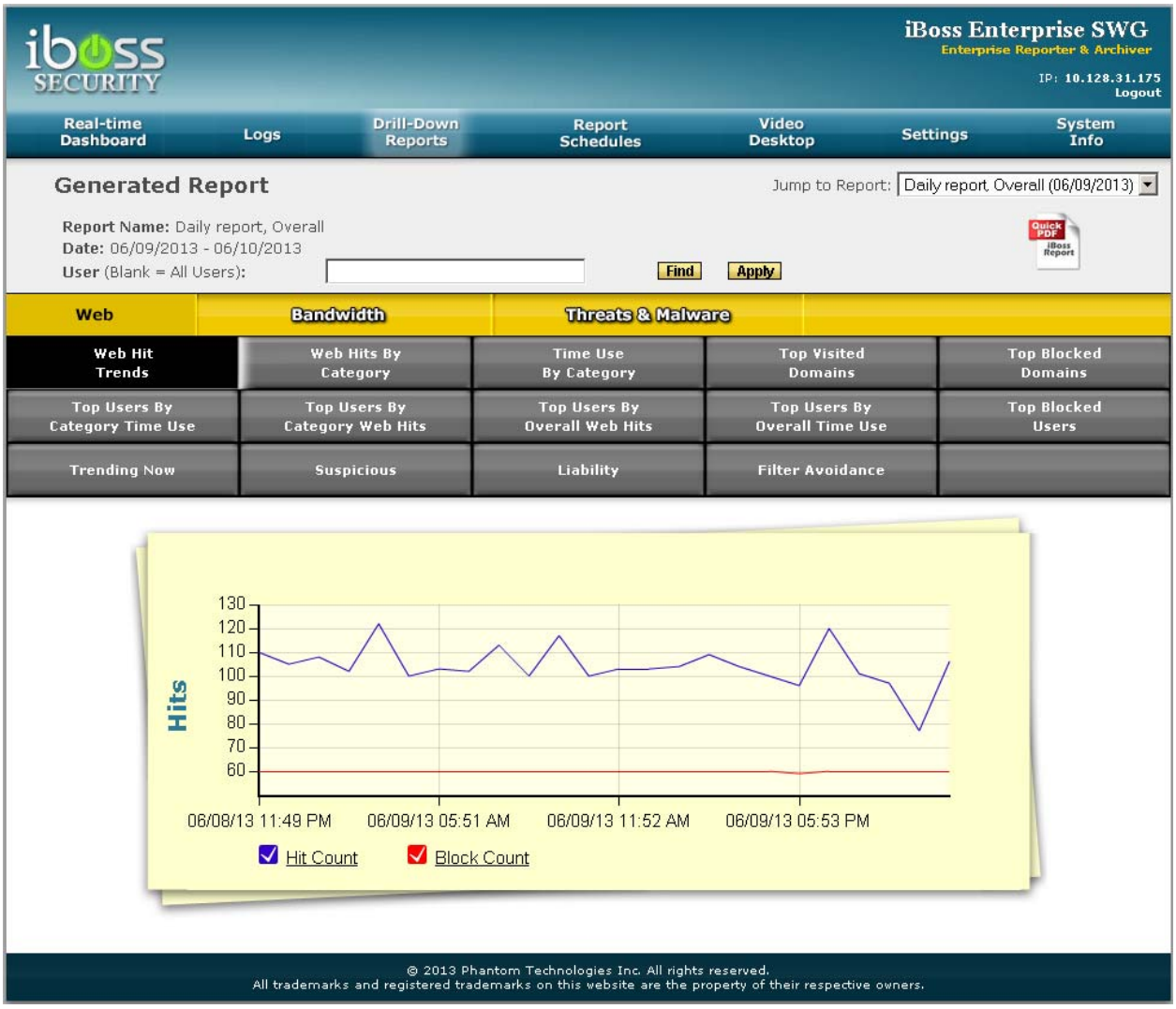


Figure 61 – Web Hit Trends

1.5.2.2 Web Hits By Category

This section shows overall web category usage by hits. It displays both total accesses and blocked accesses relative to each other. You can double-click on any of these bars to drill-down and get more detail about the particular category usage.

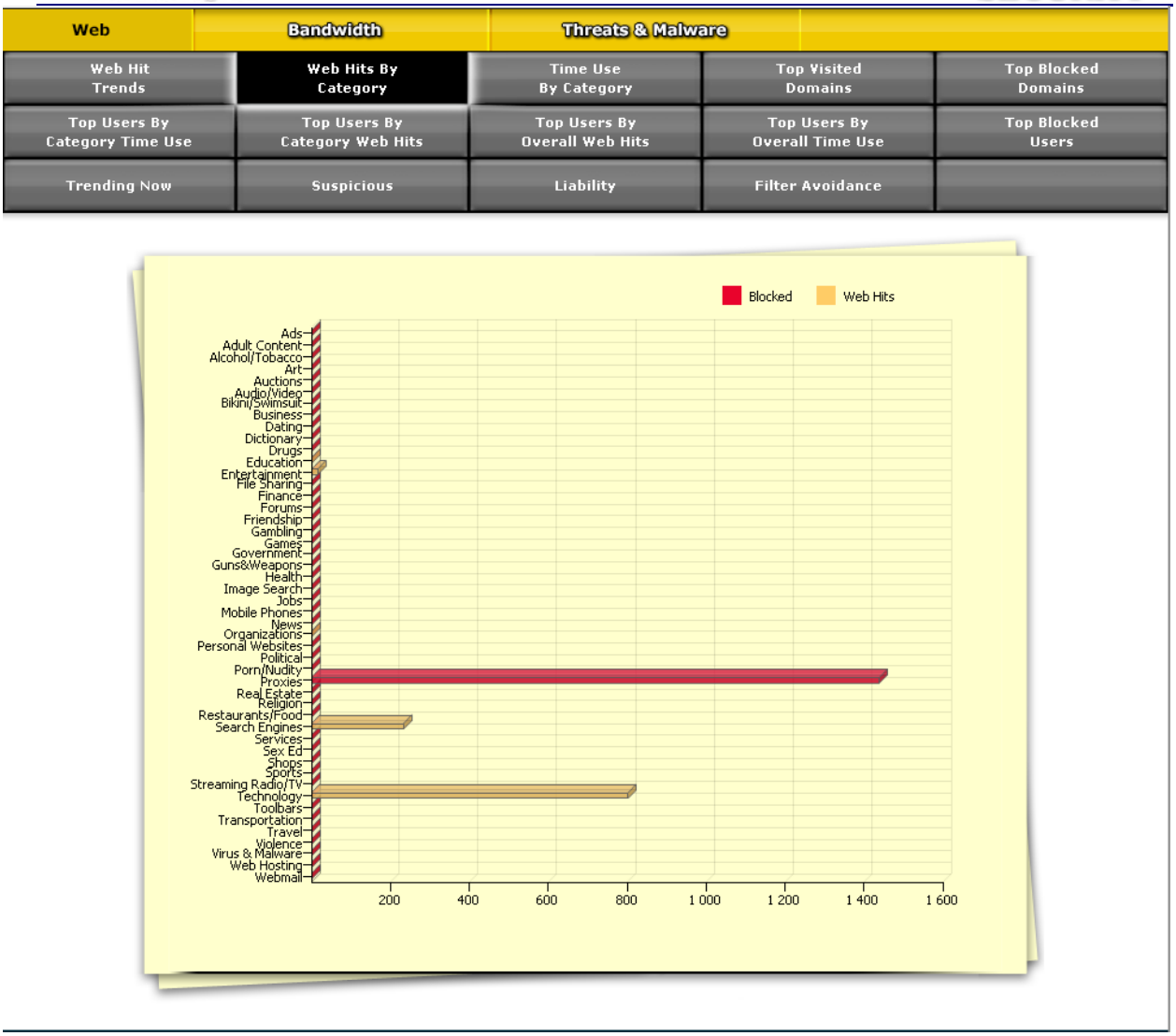


Figure 62 – Web Hits by Category

1.5.2.2.1 *Web Category Detail*

If you click on the bar for a particular web category, you are taken to a detail page showing information pertaining to that particular category.

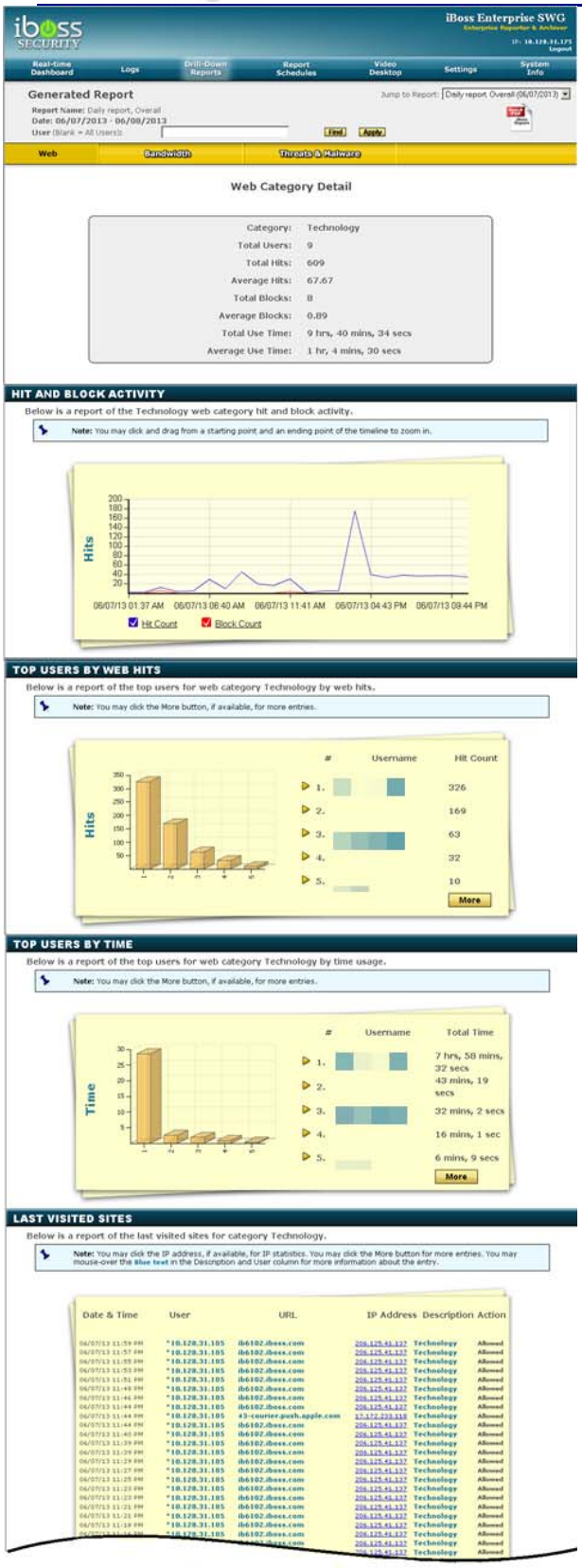

iBoss Enterprise SWG
Real-time Dashboard
Logs
Drill-Down Reports
Report Schedules
Video Desktop
Settings
System Info
Generated Report
Report Name: Daily report, Overall
Date: 06/07/2013 - 06/08/2013
User (Blank = All Users):
Find
Apply
Web
Bandwidth
Threats & Malware
Web Category Detail
Category: Technology
Total Users: 9
Total Hits: 609
Average Hits: 67.67
Total Blocks: 8
Average Blocks: 0.89
Total Use Time: 9 hrs, 40 mins, 34 secs
Average Use Time: 1 hr, 4 mins, 30 secs
HIT AND BLOCK ACTIVITY
Below is a report of the Technology web category hit and block activity.
Note: You may click and drag from a starting point and an ending point of the timeline to zoom in.
Hits
06/07/13 01:37 AM
06/07/13 08:40 AM
06/07/13 11:41 AM
06/07/13 04:43 PM
06/07/13 09:44 PM
Hit Count
Block Count
TOP USERS BY WEB HITS
Below is a report of the top users for web category Technology by web hits.
Note: You may click the More button, if available, for more entries.
Username Hit Count
1. 326
2. 169
3. 63
4. 32
5. 10
More
TOP USERS BY TIME
Below is a report of the top users for web category Technology by time usage.
Note: You may click the More button, if available, for more entries.
Username Total Time
1. 7 hrs, 58 mins, 32 secs
2. 43 mins, 19 secs
3. 32 mins, 2 secs
4. 16 mins, 1 sec
5. 6 mins, 9 secs
More
LAST VISITED SITES
Below is a report of the last visited sites for category Technology.
Note: You may click the IP address, if available, for IP statistics. You may click the More button for more entries. You may mouse-over the Blue text in the Description and User column for more information about the entry.
Date & Time User URL IP Address Description Action

Figure 63 - Web Category Detail

1.5.2.2.1.1 Hit and Block Category Detail Graph

The Hit and Block Activity graph show the activity for the currently selected category. This will give you an indication of use throughout the report period for the category selected. Remember, the information reflected on this page and the graph, pertain to either the currently selected user or all users if that option is selected in the report information section at the top.

1.5.2.2.1.2 Top Users for Web Category

This section lists the top users for the selected category. Users are ordered by highest hit count first. Click on the “More” button to get a full list of users for this category. The full list can be sorted by a variety of parameters.

1.5.2.2.1.3 Last Visited Sites

This section lists the sites in recent order of this web category.

1.5.2.3 Time Use By Category

This section shows you the top categories based on time usage. This will also show you in Hours, Minutes, and seconds of the amount of time spent on each category. You may press the expand button to see the Top 5 Users for a specific category.

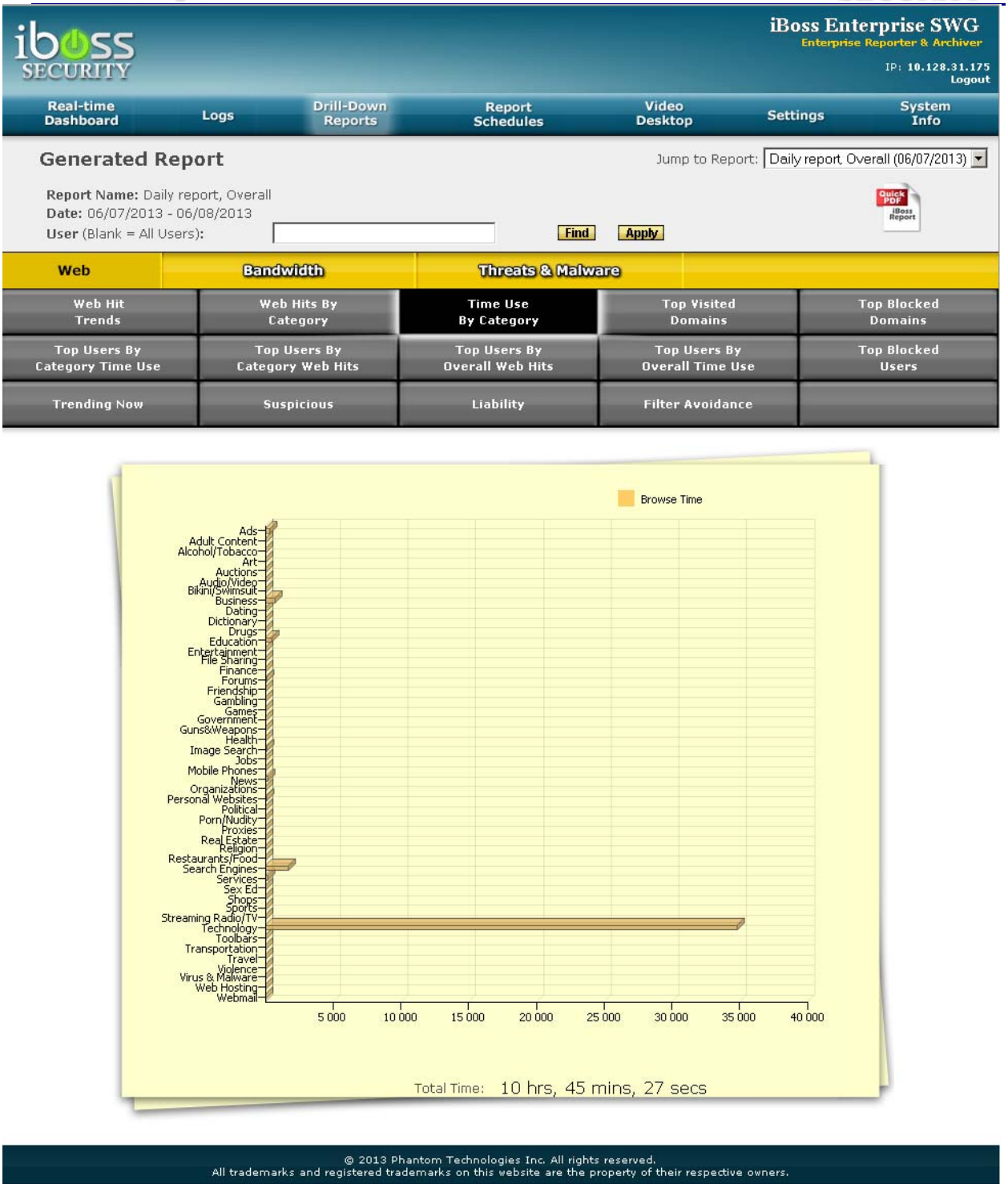


Figure 64 - Time Use By Category

1.5.2.4 Top Visited Domains

This section lists the top visited domains as well as the top blocked domains. You get a full list of domains with the ability to sort by a variety of parameters by clicking on the “More” button.

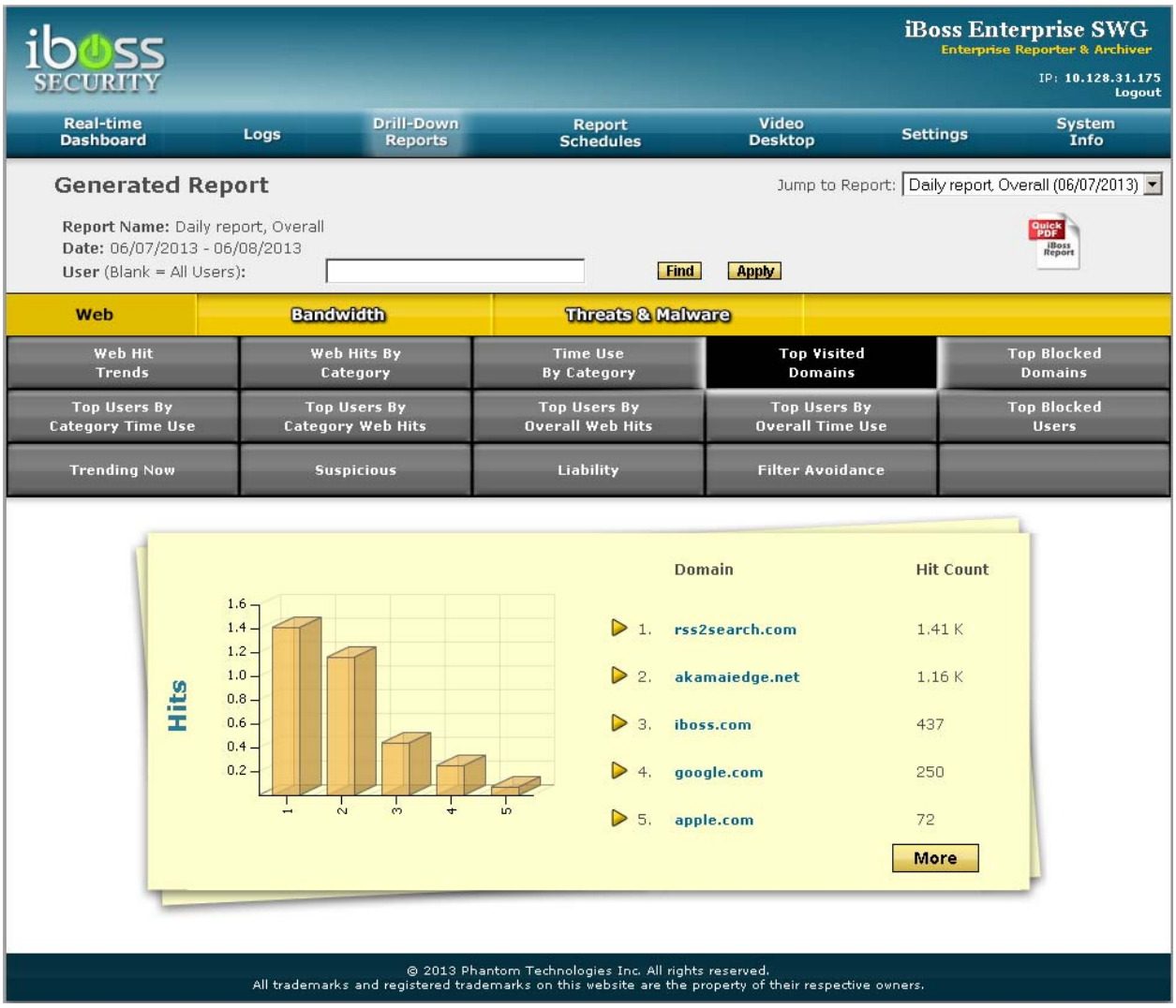


Figure 65 – Top Visited Domains

1.5.2.5 Top Blocked Domain

This section lists the top visited domains as well as the top blocked domains. You get a full list of domains with the ability to sort by a variety of parameters by clicking on the “More” button.

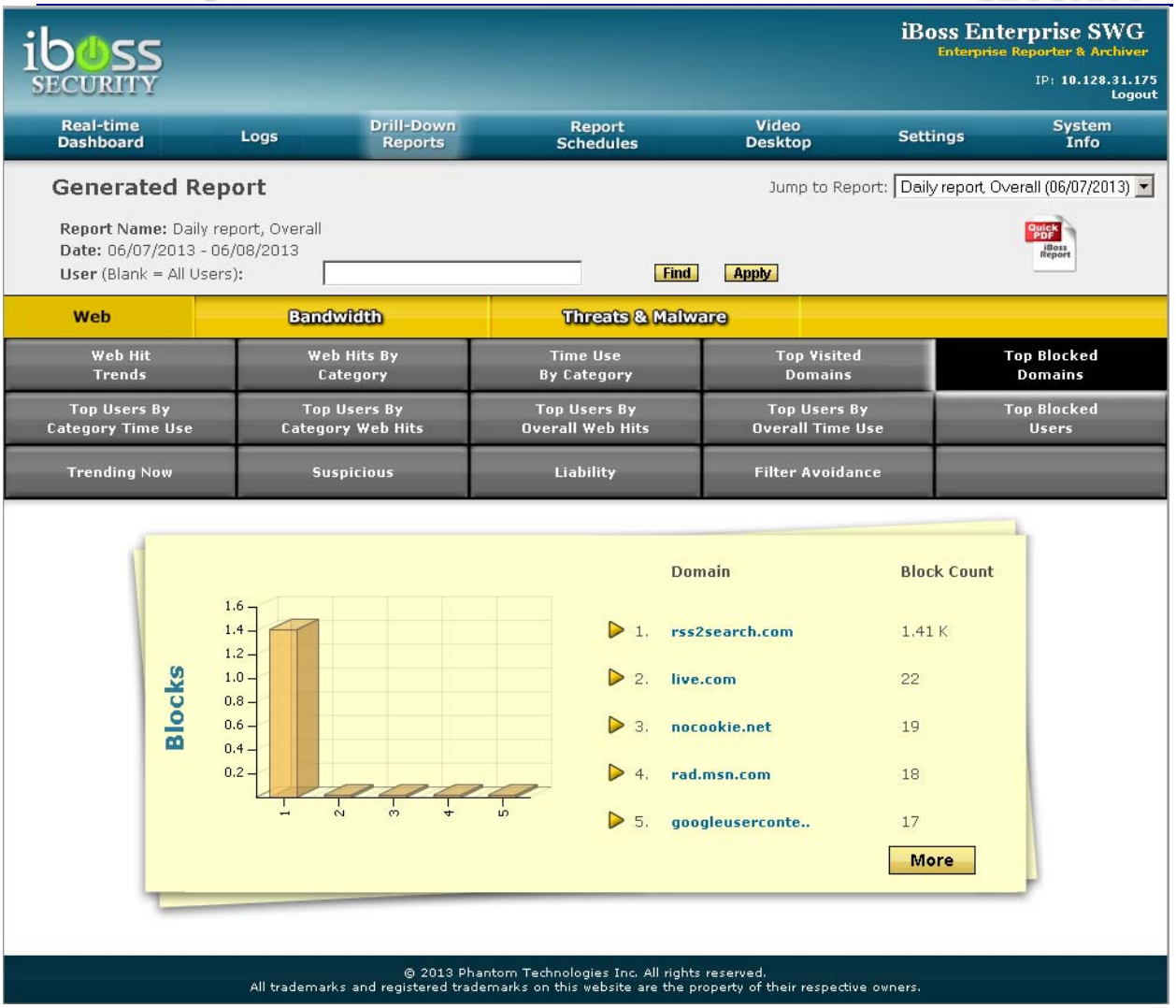
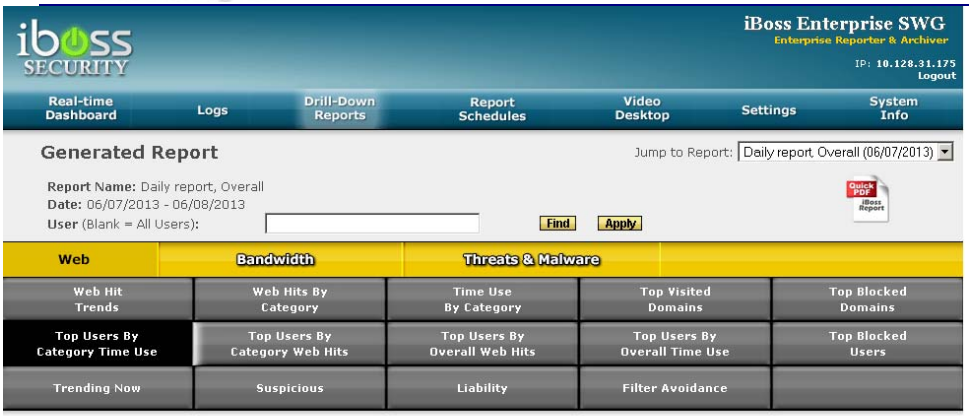


Figure 66 – Top Blocked Domains

1.5.2.6 Top Users By Category Time Use

This section lists categories and allows you to expand to show the top five users for each category by time use. You may click the More button to show all users for a specific web category. Note: If a User is selected, this field will not show.



Category (Expand All / Collapse All)	Time	
Ads	6 mins, 1 sec	More
Adult Content	0 Seconds	More
Alcohol/Tobacco	0 Seconds	More
Art	0 Seconds	More
Auctions	0 Seconds	More
Audio/Video	0 Seconds	More
Bikini/Swimsuit	0 Seconds	More
Business	12 mins, 9 secs	More
Dating	0 Seconds	More
Dictionary	0 Seconds	More
Drugs	0 Seconds	More
Education	7 mins, 31 secs	More
Entertainment	2 secs	More
File Sharing	0 Seconds	More
Finance	0 Seconds	More
Forums	1 min, 24 secs	More
Friendship	0 Seconds	More
Gambling	0 Seconds	More
Games	0 Seconds	More
Government	0 Seconds	More
Guns&Weapons	0 Seconds	More
Health	0 Seconds	More
Image Search	1 min, 24 secs	More
Jobs	0 Seconds	More
Mobile Phones	0 Seconds	More
News	3 mins, 17 secs	More
Organizations	0 Seconds	More
Personal Websites	1 min, 24 secs	More
Political	0 Seconds	More
Porn/Nudity	0 Seconds	More
Proxies	0 Seconds	More
Real Estate	0 Seconds	More
Religion	0 Seconds	More
Restaurants/Food	0 Seconds	More
Search Engines	28 mins, 29 secs	More
Services	3 mins, 8 secs	More
Sex Ed	0 Seconds	More
Shops	0 Seconds	More
Sports	0 Seconds	More
Streaming Radio/TV	0 Seconds	More
Technology	9 hrs, 40 mins, 34 secs	More
Toolbars	0 Seconds	More
Transportation	0 Seconds	More
Travel	0 Seconds	More
Violence	0 Seconds	More
Virus & Malware	0 Seconds	More
Web Hosting	4 secs	More
Webmail	0 Seconds	More

Total Time: 17 hrs, 34 mins, 31 secs

© 2013 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 67 – Top Users by Category Time Use

1.5.2.7 Top Users By Category Web Hits

This section lists categories and allows you to expand to show the top five users for each category by web hits. You may click the More button to show all users for a specific web category. Note: If a User is selected, this field will not show.

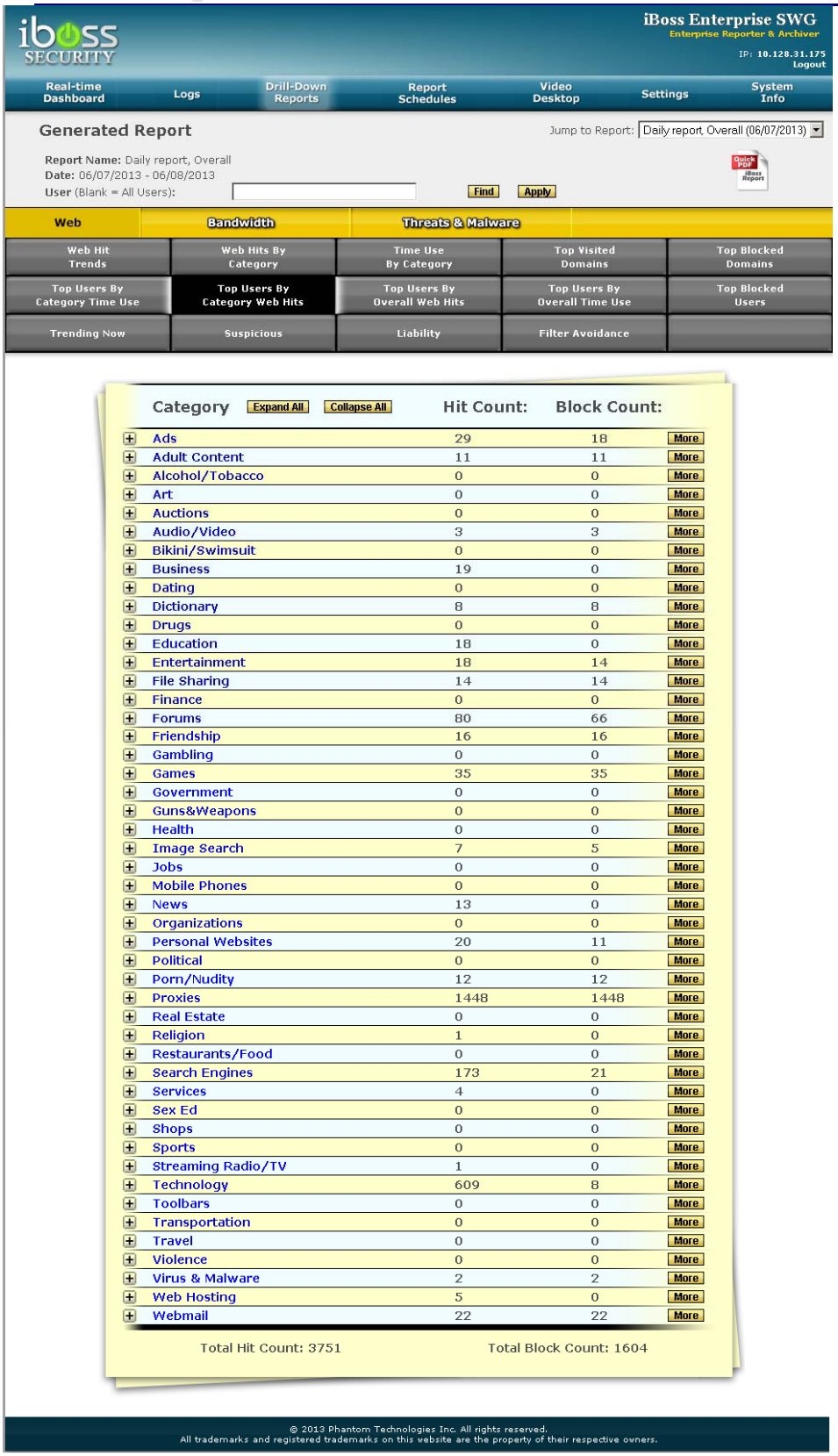


Figure 68 – Top Users by Category Web Hits

1.5.2.8 Top Users By Overall Web Hits

This section lists the top five users by overall web hits. You may click the More button to show all users listed by web hits.

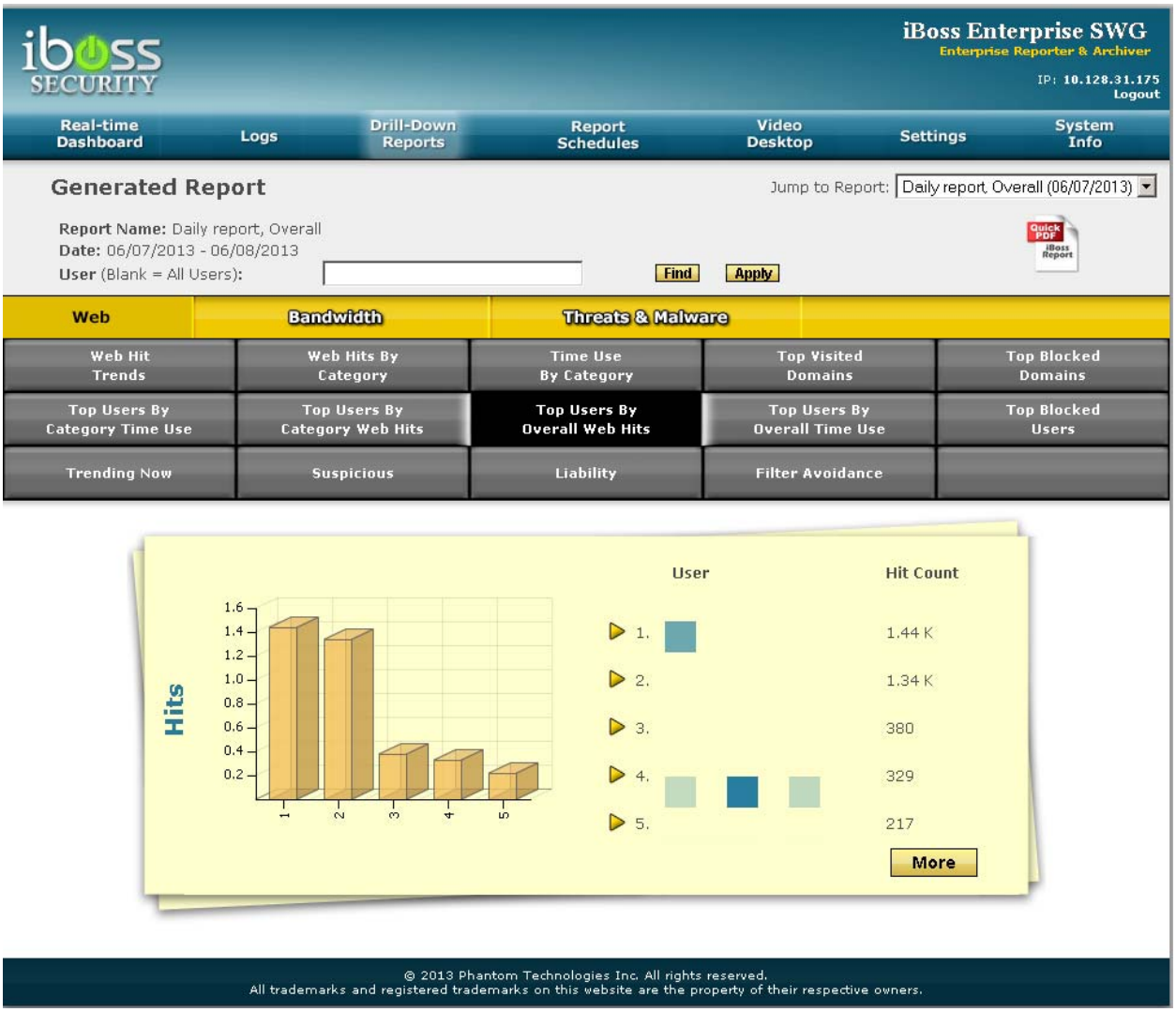


Figure 69 - Top Users By Overall Web Hits

1.5.2.9 Top Users By Overall Time Use

This section lists the top five users by overall time use. You may click the More button to show all users listed by over time use.

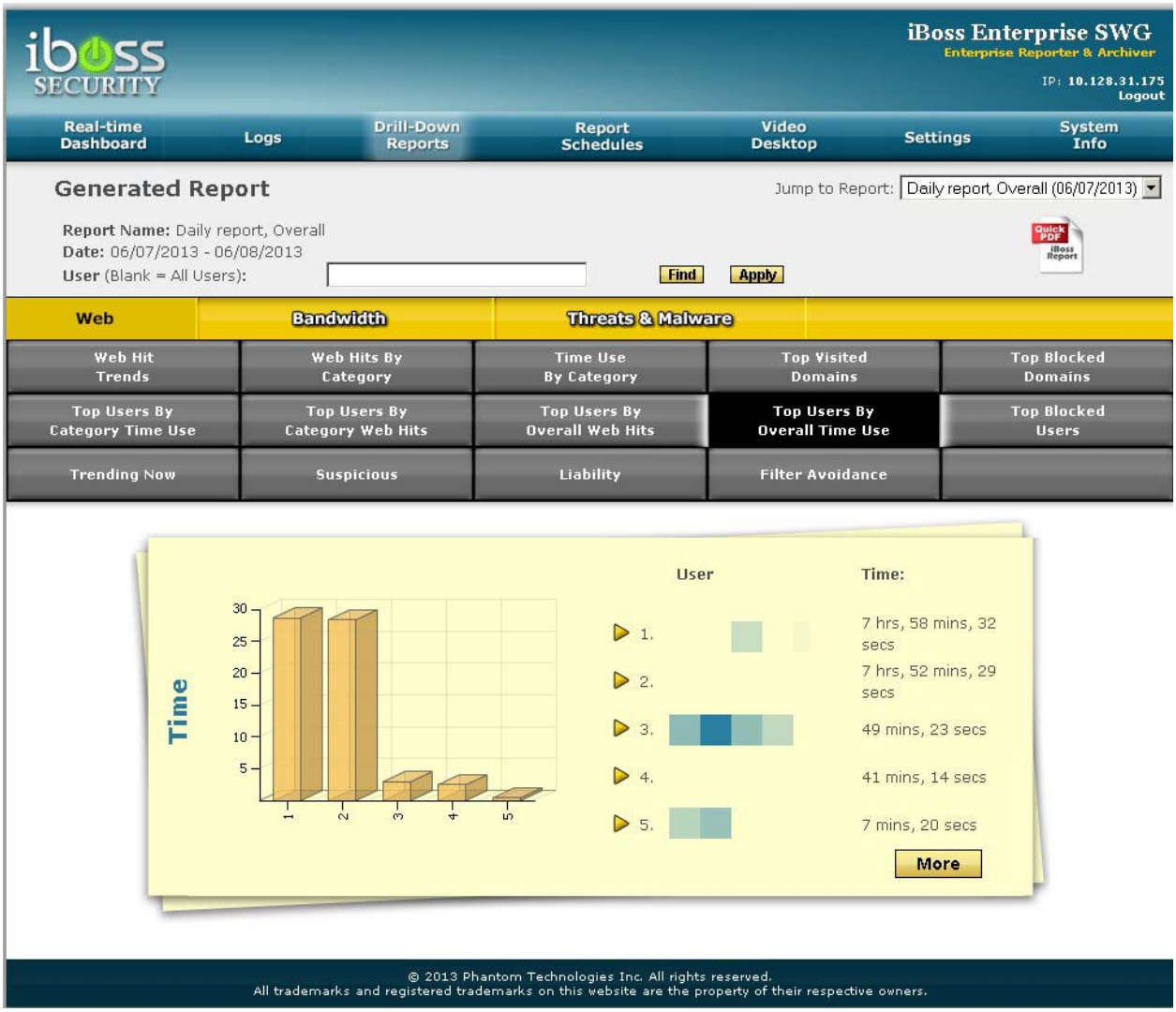


Figure 70 - Top Users by Overall Time Use

1.5.2.10 Top Blocked Users

This section lists the top five blocked users. You may click the More button to show all users listed by block count.

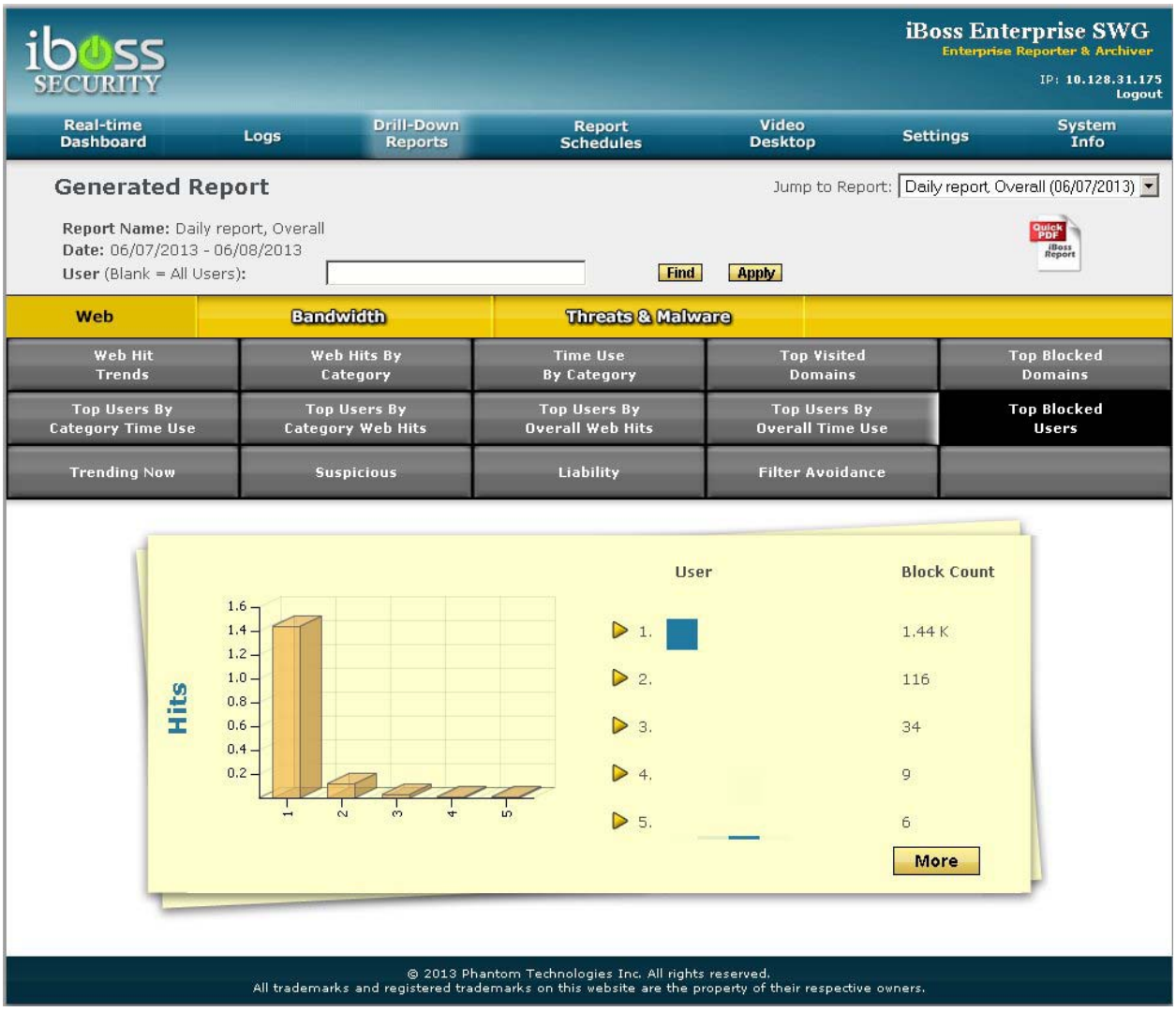


Figure 71 – Top Blocked Users

1.5.2.11 Trending Now

This section details the top searches on your network. The “More” button brings up a full list of search terms.

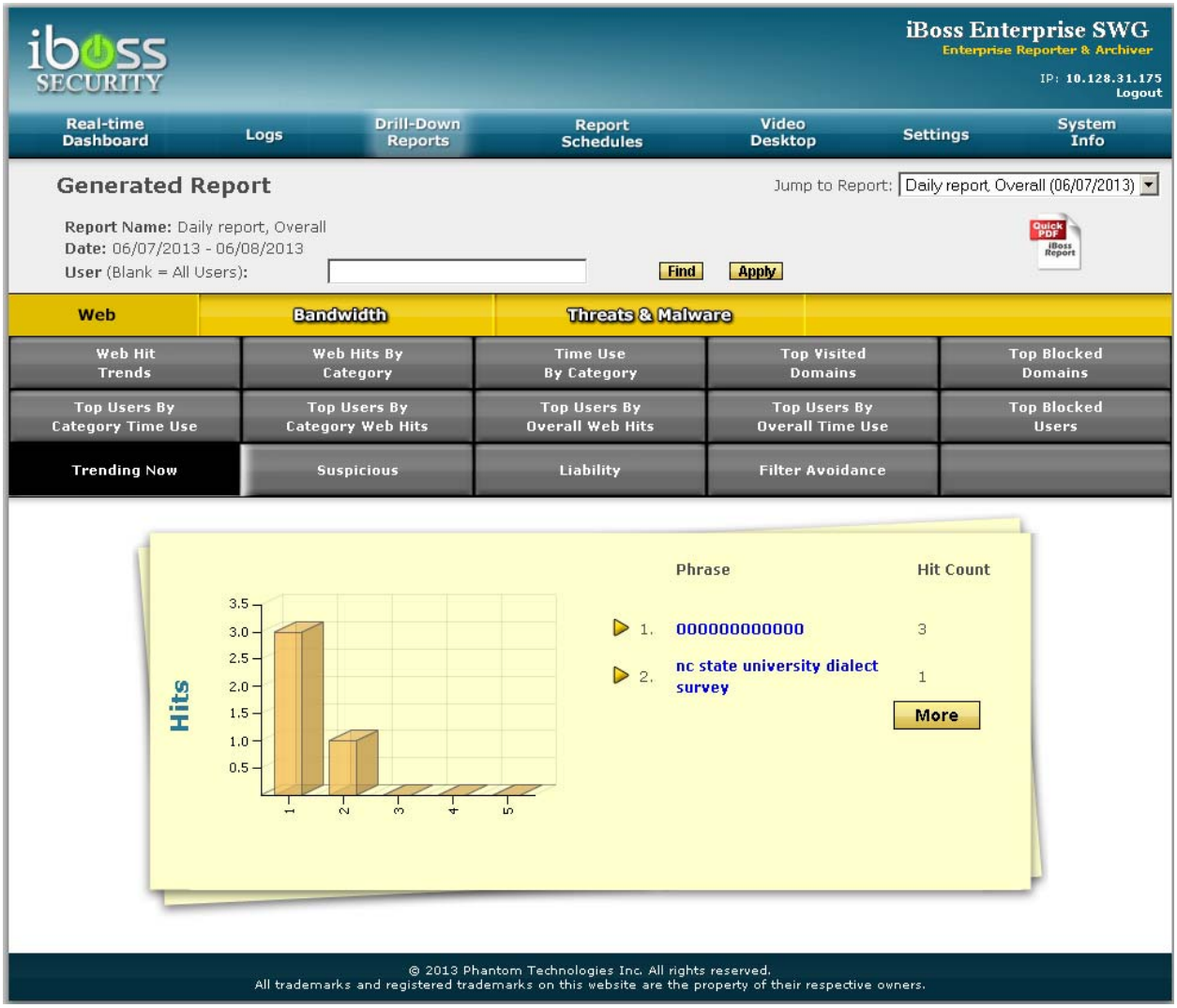


Figure 72 – Trending Now

1.5.2.12 Suspicious

This section lists searches that match words on the Suspicious word list. The “Edit Words” button opens the list for editing.

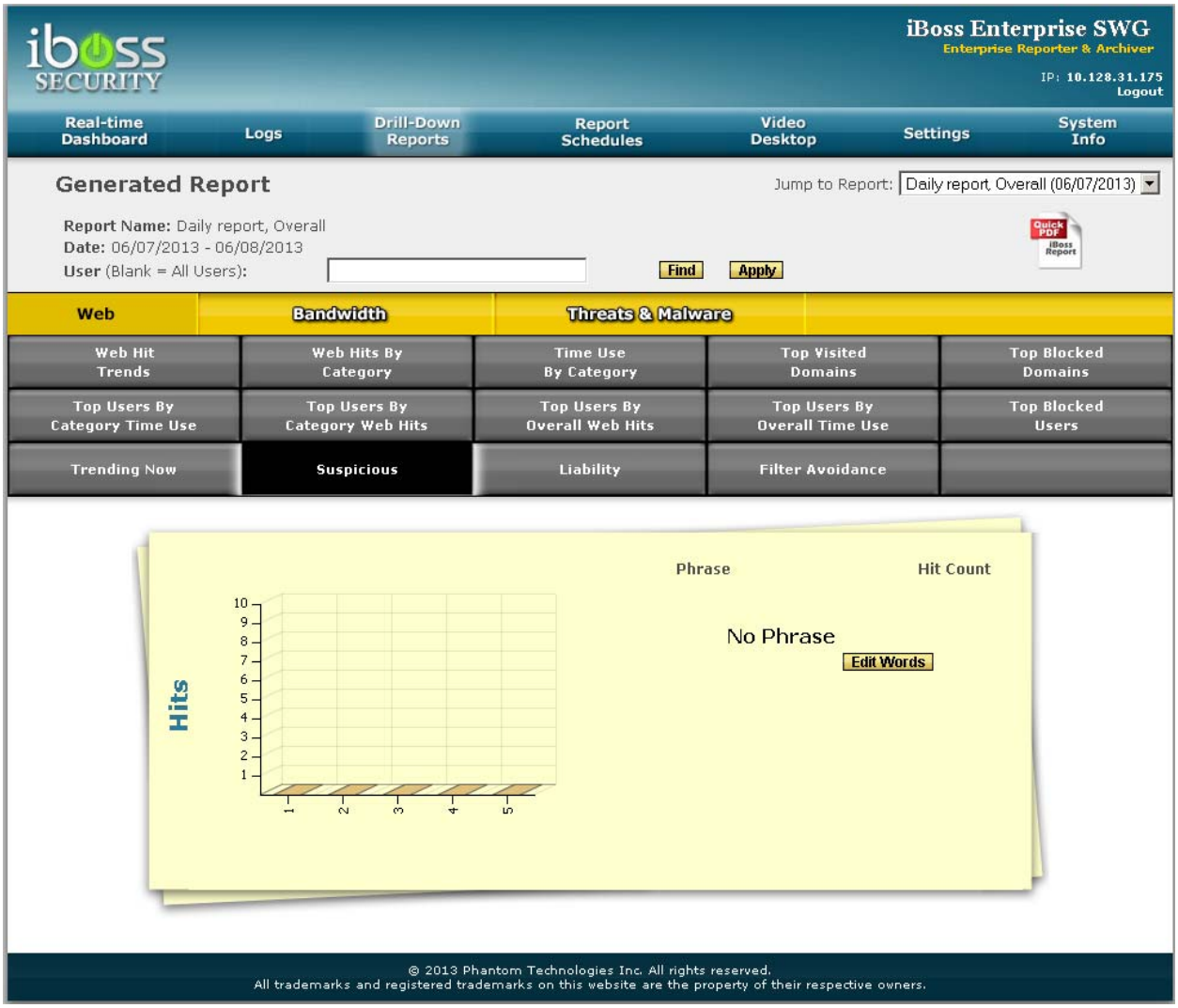


Figure 73 – Suspicious

1.5.2.13 Liability

This section lists searches that match words on the Liability word list. The “Edit Words” button opens the list for editing.

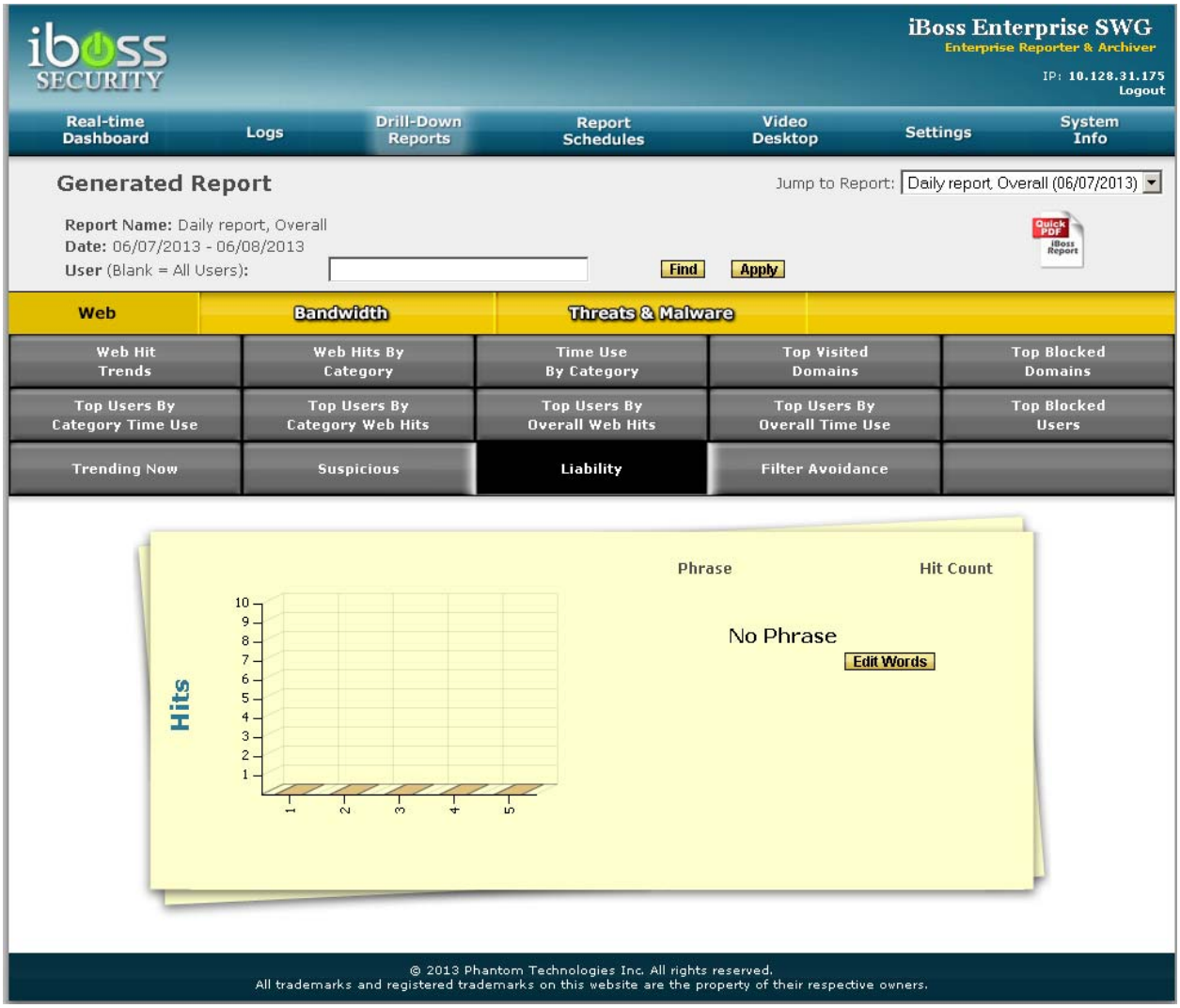


Figure 74 – Liability

1.5.2.14 Filter Avoidance

This section lists searches that match words on the Filter Avoidance word list. The “Edit Words” button opens the list for editing.

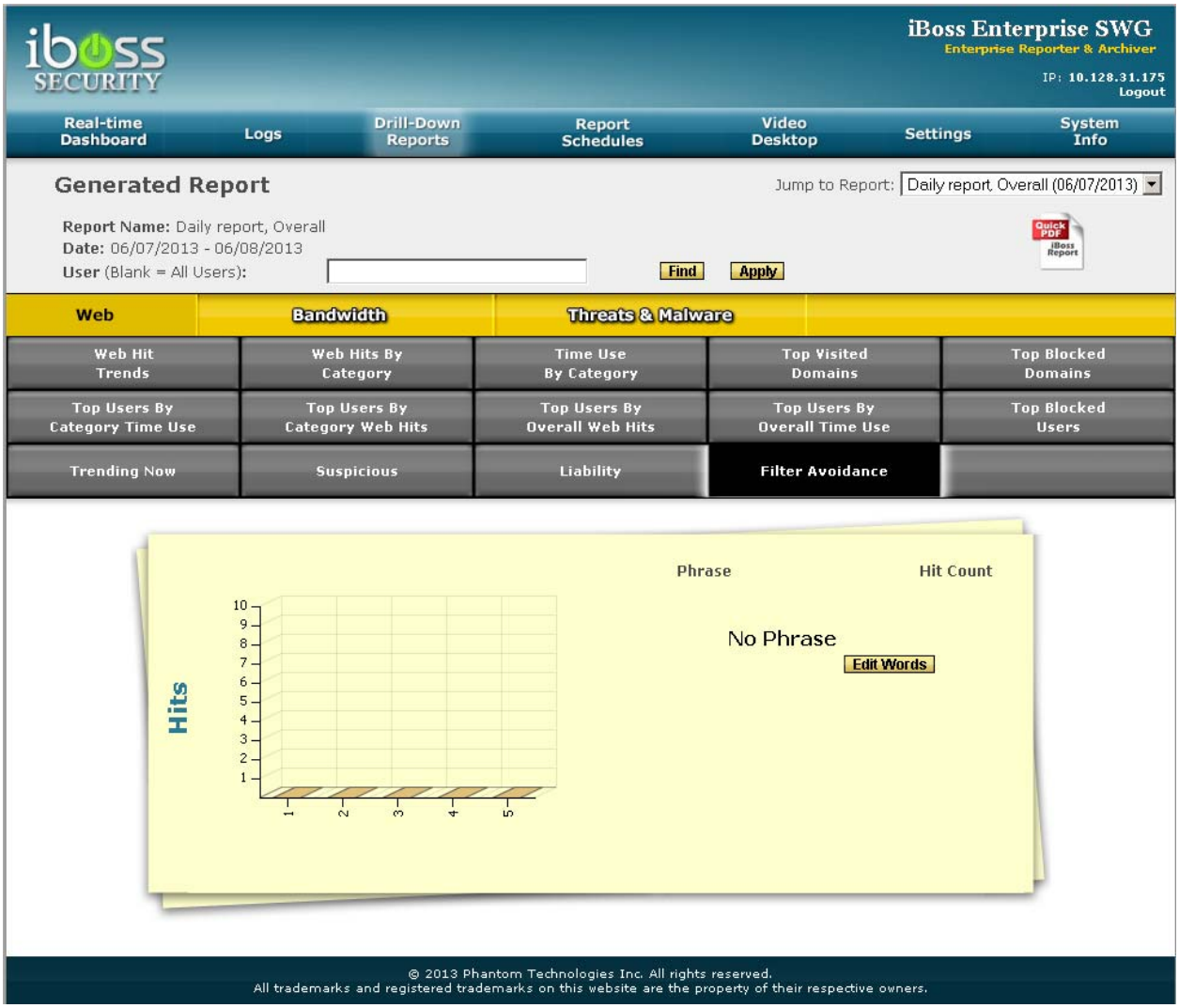


Figure 75 – Filter Avoidance

1.5.3 Bandwidth Statistics

The Bandwidth statistic section provides information regarding general bandwidth usages from your network. General bandwidth includes overall, downstream and upstream usage.

1.5.3.1 Graph

This graph shows the total bandwidth activity throughout the report period.

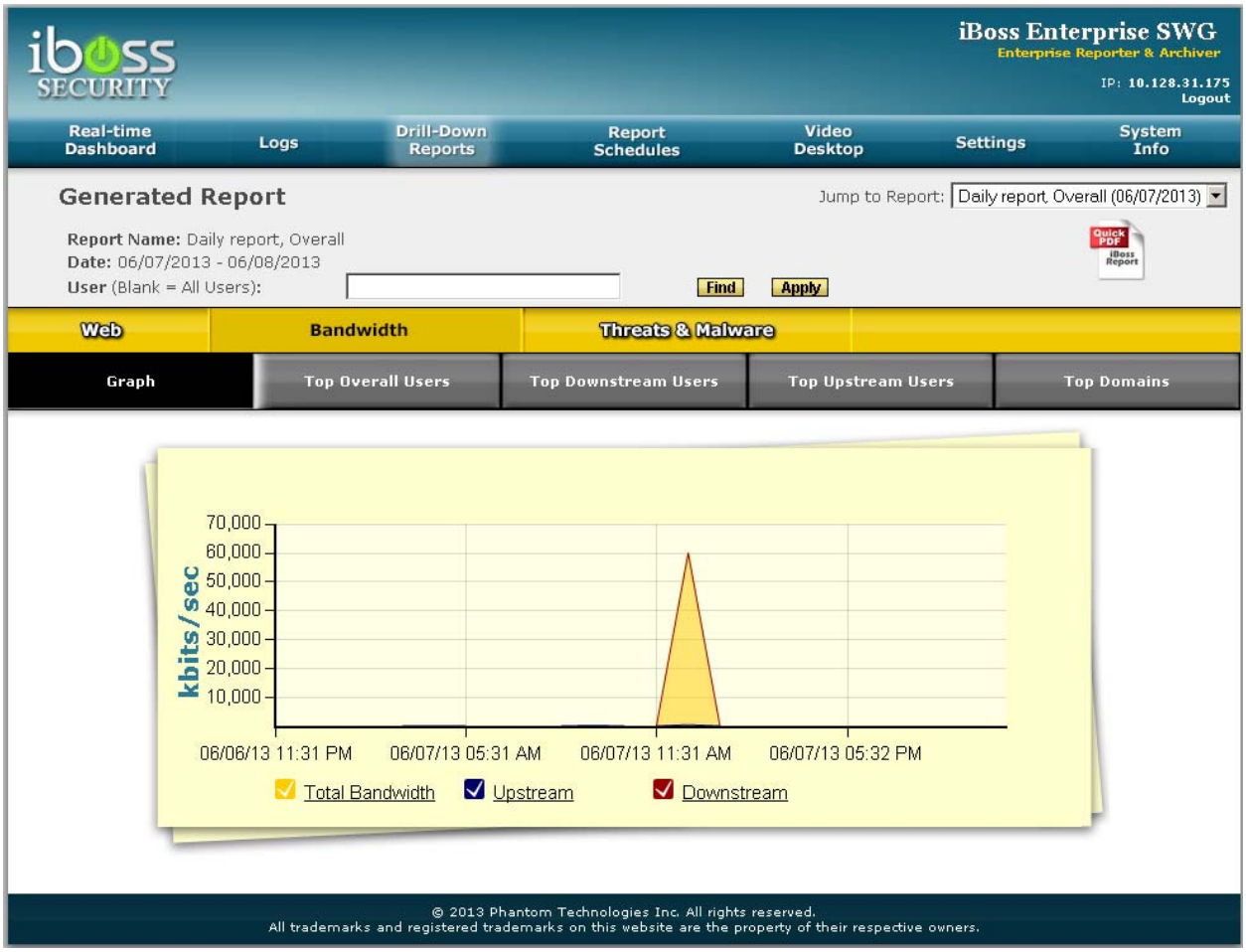


Figure 76- Graph

1.5.3.2 Top Overall Users

This graph shows the top 5 bandwidth users. Clicking the MORE button gives a complete list.

Figure 77 – Top Bandwidth Users

1.5.3.3 Top Downstream Users

This graph shows the top 5 downstream bandwidth users. Clicking the MORE button gives a complete list.

Figure 78 – Top Downstream Users

1.5.3.4 Top Upstream Users

This graph shows the top 5 upstream bandwidth users. Clicking the MORE button gives a complete list.

Figure 79 – Top Upstream Users

1.5.3.5 Domains

This section contains the top five domains by bandwidth usage. You may click the More button for a full list.

Figure 80 – Domains

1.5.4 Threats & Malware

The Threats & Malware section provides information from IPS units that are attached to the Reporter. Please refer to the IPS Guide for more information.

1.5.4.1 Top Overall Threats

This section contains the top overall threats as determined by the IPS. You may click the More button for a full list.

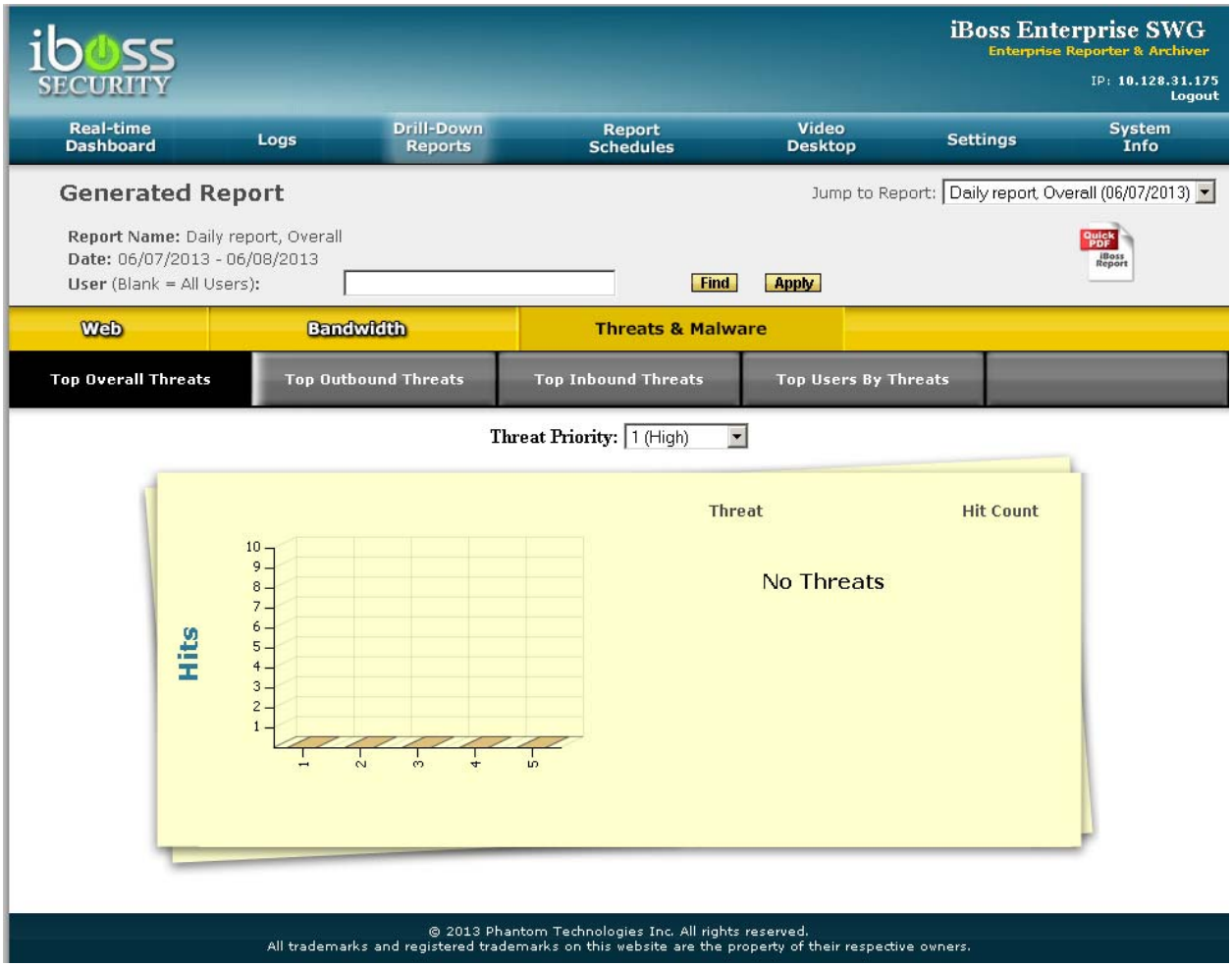


Figure 81 – Top Overall Threats

1.5.4.2 Top Outbound Threats

This section contains the top outbound threats as determined by the IPS. You may click the More button for a full list.

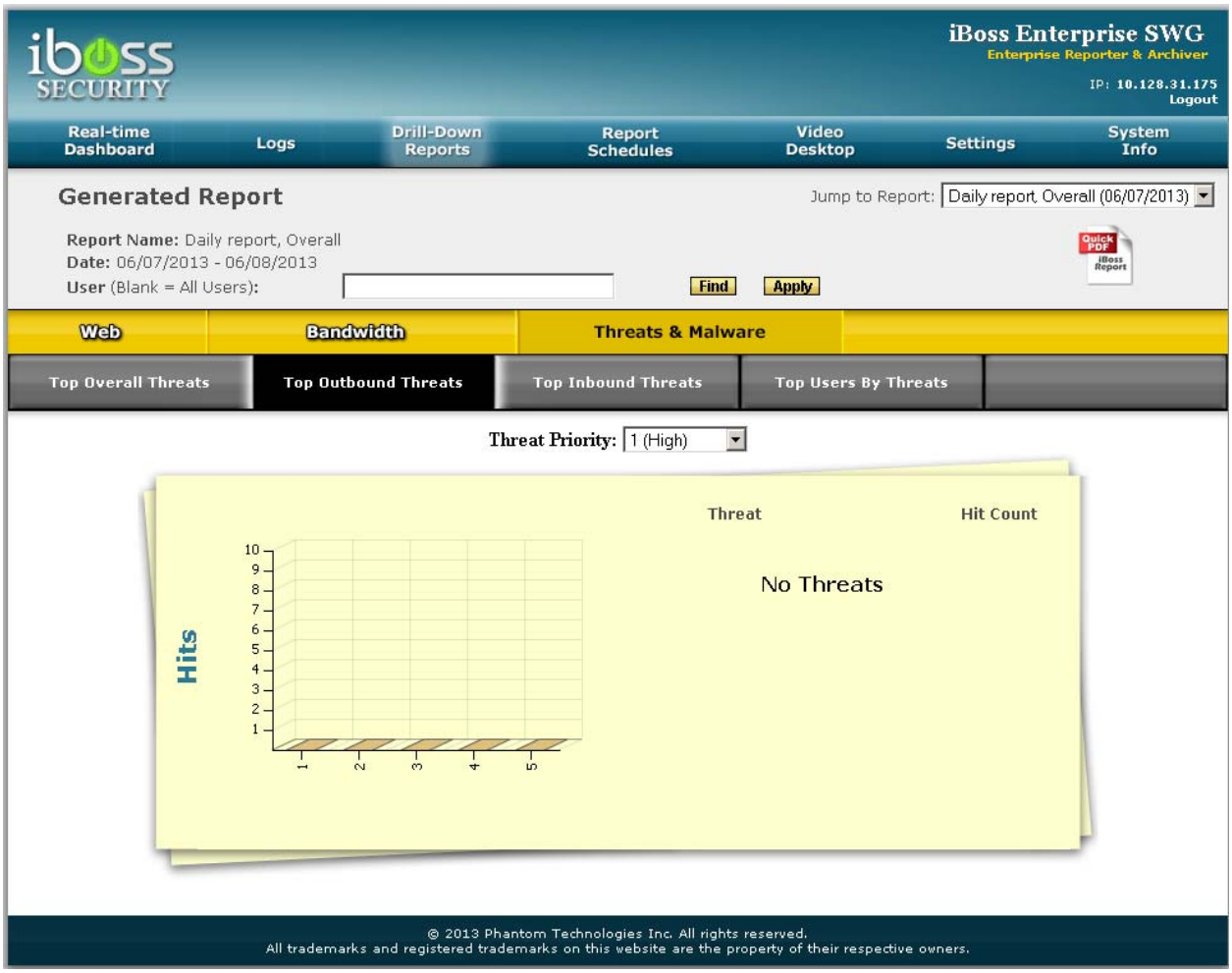


Figure 82 – Top Outbound Threats

1.5.4.3 Top Inbound Threats

This section contains the top inbound threats as determined by the IPS. You may click the More button for a full list.

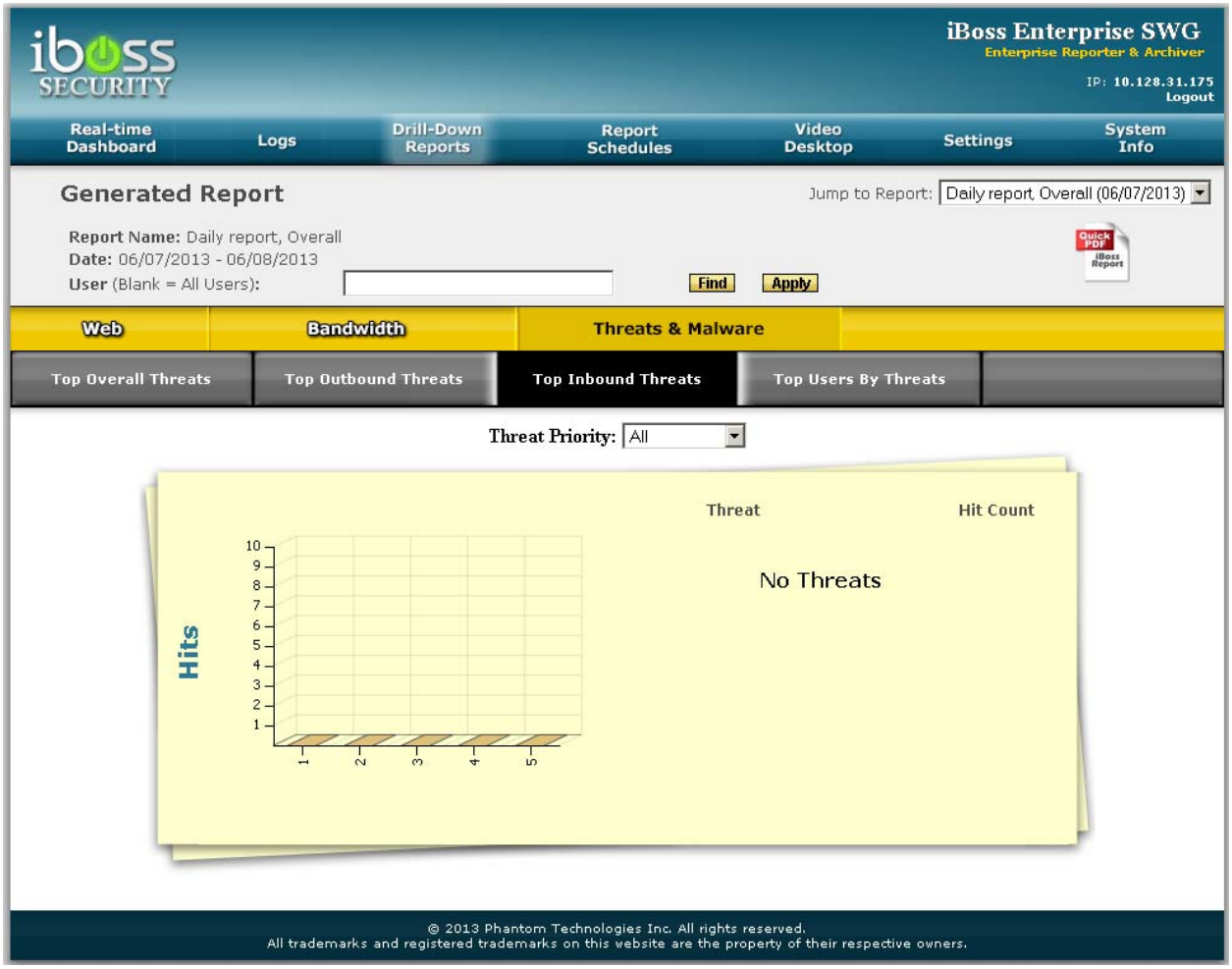


Figure 83 – Top Inbound Threats

1.5.4.4 Top User by Threats

This section contains the top users by threats as determined by the IPS. You may click the More button for a full list.

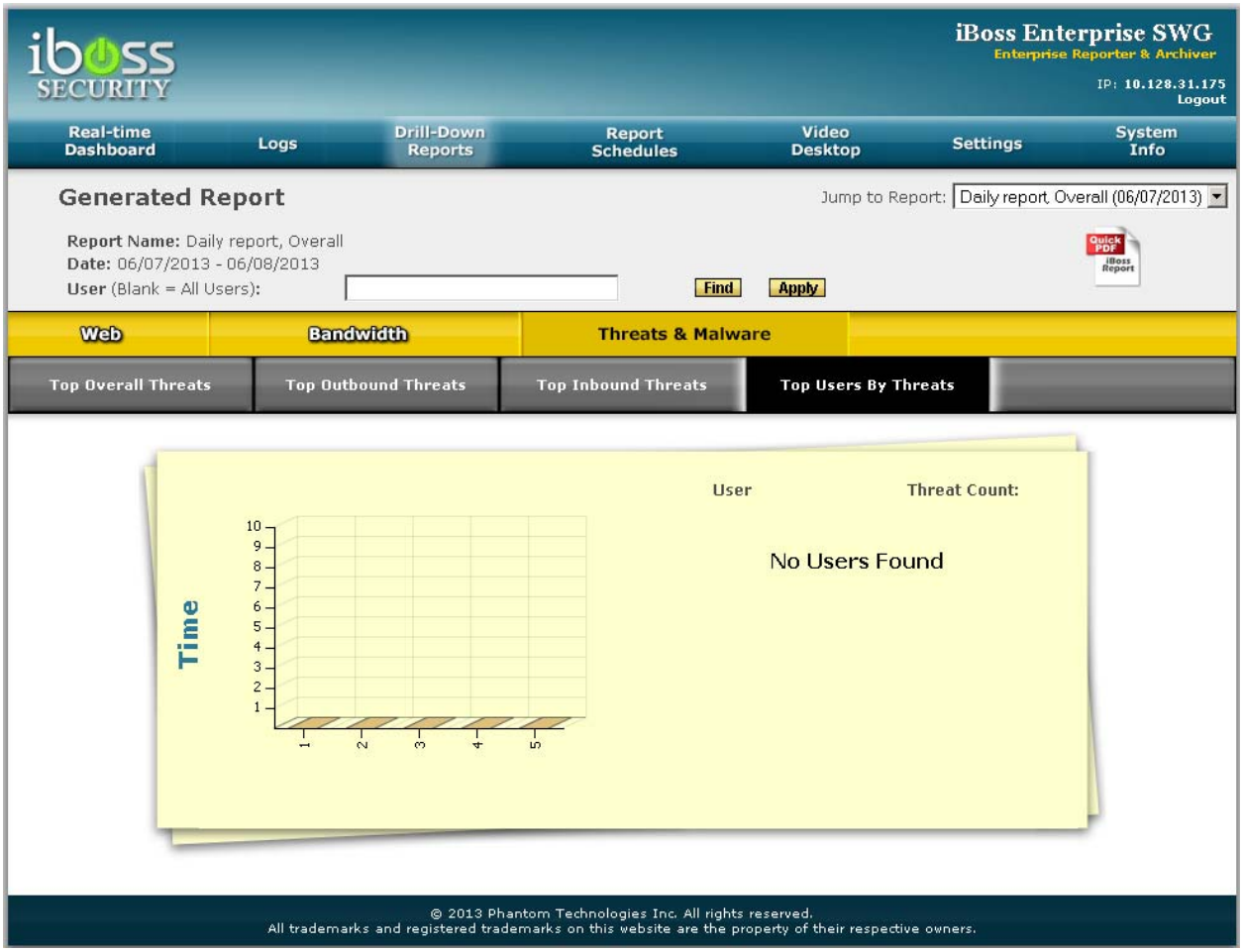


Figure 84 – Top Users by Threats

2 REGULATORY STATEMENT

FCC
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC rules.

CE
This equipment has been tested and found to comply with the limits of the European Council Directive on the approximation of the law of the member states relating to electromagnetic compatibility (89/336/EEC) according to EN 55022 Class B.

FCC and CE Compliance Statement
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Safety
This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment.